

Cybersecurity Talent Shortage

Silvana Tomić Rotim, University of Applied Sciences Velika Gorica, Velika Gorica, Croatia
Višnja Komnenić, ZIH d.o.o., Zagreb, Croatia

Address for correspondence: Silvana Tomić Rotim, University of Applied Sciences Velika Gorica, Velika Gorica, Croatia, e-mail: stomic@zih.hr

Abstract

Different reports show that organizations face a number of hurdles in their efforts to better protect sensitive data. Most frequently mentioned is the challenge of enforcing security policy across the data lifecycle (57%), followed by lack of expert staff (50%), and lack of budget (48%). This article includes the statistics regarding cybersecurity threats and attacks, professionals' shortage and the expected knowledge, skills and experience for doing this kind of job. Also the article offers some possible solutions for solving this problem, as well as the advantages and disadvantages of different options.

Keywords

Cybersecurity, Cybersecurity attacks, Cybersecurity threats, skills shortage, MSSP - Managed Security Service Provider

1. Introduction

According to the International Information System Security Certification Consortium, (ISC)², the world is facing the shortage of Cybersecurity experts of 2.93 million (Richards, 2018). Many organizations recognize it as the most important challenge in their everyday efforts for protecting information asset, especially the sensitive one from the Cybersecurity attacks. Different statistics regarding this issue are presented in this paper. Based on the analysis of the different statistics and practices we tried to identify the best possible solutions for answering to this challenge of Cybersecurity talents shortage.

It could be considered either as a shortage of people with Cybersecurity skills or as issues with the hiring processes that which asks candidates for formal certificates, not their commitment and willingness to work. Because of that the paper covers the most important knowledge and certificates that are expected from the experienced Cybersecurity experts in order to successfully tackle the problem with Cybersecurity attacks.

2. Problem description

In the last decades a lot of organizations have experienced different types of Cybersecurity attacks, such as Ransomware, Internet of Things Botnets, Phishing and Whaling attacks, Business Process Compromise Attacks, Machine Learning enabled attacks etc. (Goud, 2017).

A Cybersecurity attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. A Cybersecurity attack can maliciously disable computers, steal data, or use breached computers as a launch point for other attacks. Cybercriminals use a variety of methods

to launch a Cybersecurity attack, including malware, phishing, ransomware, denial of service, among other methods.

The most dangerous Cybersecurity threats or attacks over the three years according to Intel Security Report are shown in the Table 1.

Table 1. The most dangerous Cybersecurity threats or attacks

No	2017	2018	2019
1	Ransomware	Ghostly Crypto-mining	Ecuador Cyber Attack
2	Internet of Things Botnets	Trick or Treat	Data Leak of First American Corporation 885,000,000 attacked files
3	Phishing and Whaling attacks	Hackers to go super advanced	Oklahoma Department of Securities
4	Business Process Compromise Attacks	A major threat to Cloud	Trendmicro data breach
5	Machine Learning enabled attacks	State-funded Attacks – North Korea	Flipboard cyber attack
6			Facebook data breach, 540 million records leaked
7			Fortnite app data breach, impact on 200 million accounts

Source: Goud, N. 2017; Goud, N. 2018; Goud, N. 2019

The most dangerous Cybersecurity threats in 2017 (Goud, N. 2017), are:

Ransomware is type of malware that threatens to publish the victims' data or block access to computer unless ransom is paid.

Internet of Things Botnets is a malware that turns network devices running Linux into remotely controlled bots that can be used as a part of botnet.

Phishing and Whaling attacks is a concept where hackers send fraudulent emails from trusted accounts to target companies through staff members. When a person clicks on an email, then the attachment releases malicious software that is able to steal data.

Business Process Compromise Attacks is a kind of attacks where hackers are using techniques to manipulate the day-to-day activities of a company for their own benefits.

Machine Learning enabled attacks is technology of Artificial Intelligence that is used to launch social engineering attacks.

The most dangerous Cybersecurity threats in 2018 (Goud, N. 2018), are:

Ghostly Crypto-mining is new cyber threat. Hackers attack servers operating in data centers to mine digital currency. In the future we can expect that the subject of this kind of attacks will be individuals and their browsers.

Trick or Treat is social engineering tactics that consist of launching phishing emails with unpleasant malware.

Hackers to go super advanced - advanced malware developers develop malware that is undetectable by anti-malware solutions.

A major threat to Cloud, cloud computing is very important for many organizations, but there are a lot of possible risks in using it. The poorly configured cloud platforms and virtual storage become the subject of attacks by hackers.

State-funded Attacks is major attack launched by North Korea on Europe, Canada, United States, Australia and some parts of Asia. Its target is the critical infrastructure of government agencies.

The most dangerous Cybersecurity attacks in 2019 (Goud, N. 2019), are:

Ecuador Cyber Attack is an attack on the database with the personal information about the Ecuadorian population. More than 30 million populace and their personal data were attacked.

Data Leak of First America Corporation - hackers accessed over a three-quarter billion mortgage deal documentation. The breached data includes bank account numbers, tax records, social security numbers, etc.

Oklahoma Department of Securities – Hackers gained access to more than a million files related to several FBI investigations.

Trendmicro data breach - The hackers attacked Trendmicro's database and stole the data related to the names, email addresses, ticket numbers and contact information.

Flipboard Cyber-attack – the Internet site Flipboard has experienced two Cyber-attacks. Flipboard estimates that a data breach could affect almost all of its users.

Fortnite app data breach - gaming app Fortnite confessed that it has vulnerability in its website. This vulnerability could cause taking over more than 200.000 accounts by hackers.

Regarding mentioned all these Cybersecurity threats and attacks we can see that the one of greatest threat that business faces today is Cybersecurity specialist and talent shortage (Donegan, K., 2019). To be capable to answer to these threats or attacks, beside the technology, the organizations need experienced and educated people. It is difficult to recruit and retain the Cybersecurity experts in the company. The Nonprofit Association (ISC)² report shows that nearly three million Cybersecurity experts are currently missing, which is a serious problem. Businesses need to be aware of this problem and try to find the best way to solve it.

We can see in Croatian companies that mostly companies invest in different kind of technologies even without the extensive risk assessment and identification of the most critical risks. At the same time these companies do not have budget for developing and training of their own employees responsible for security issues or engaging the adequate external experts.

As the biggest Cybersecurity challenges according to Oltsik, J. (2019) are presented in figure 1.



Figure 1. The biggest Cybersecurity challenges

Usually Cybersecurity experts start their career as an IT professional before becoming a cybersecurity professional. Therefore, probably it would be opportune to recruit new Cybersecurity experts from IT population. The most helpful IT skills and knowledge that can be applied in Cybersecurity activities are experience with different types of technologies and applications (53%), knowledge about networking technology and other types of infrastructure (49%), and IT operations knowledge and skills (49%), and IT operations knowledge and skills, figure 2.

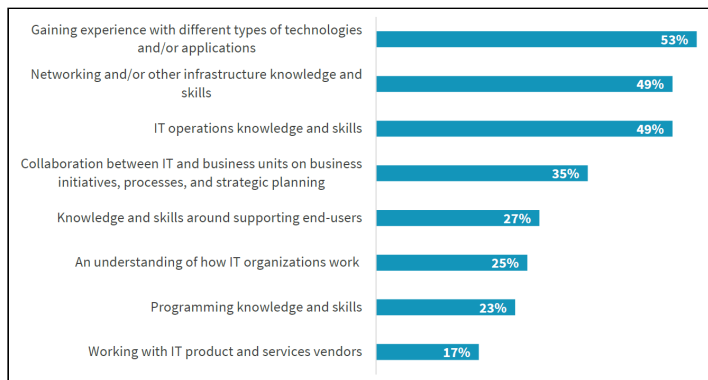


Figure 2. The most helpful IT skills and knowledge in Cybersecurity activities

Source: Oltsik, J. (2019)

For successful recruitment of IT experts and their career it is necessary to send them on different types of education and certification. According to Oltsik, J. (2019) the most important certification for Cybersecurity career is CISSP - Certified Information Systems Security Professional (45%), figure 3.

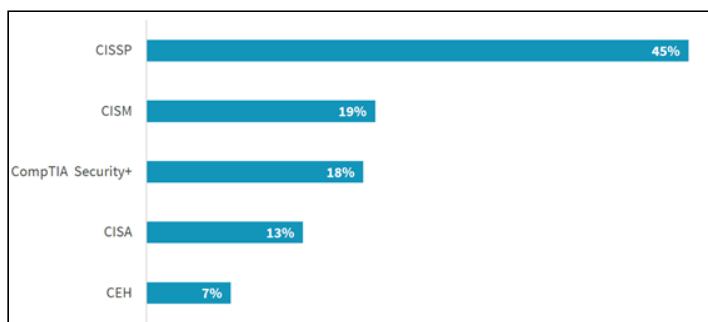


Figure 3. The most important certifications for Cybersecurity career

The other very important problem is the fact that that two-thirds of security professionals have considered leaving their current positions or the industry entirely, Donegan, K. (2019). One reason for that is a lack of skills for solving different issues regarding Cybersecurity, and the other one is a lack of capabilities and willingness for continuous learning and improving their skills.

3. Possible Solutions

Based on the above presented analysis and statistics, we can conclude that there are three possible solutions for solving a problem described in the paragraph 2 of this paper. The first option is looking for the certified and experienced cybersecurity experts and keeping them well educated and trained during their employment. This option could cost a lot because it requires investing a lot of money in employees responsible for information security in all domains: managerial, organizational, legal and technical. It is also almost impossible to maintain the expected level of knowledge in all mentioned domains if the companies do not have adequate number of team members, not just a person for security issues. Therefore, mostly big companies choose this solution for solving their Cybersecurity problems. There are different opinions regarding the most effective methods of improving knowledge and skills necessary for answering to all challenges in Cybersecurity. According to Oltsik, J. (2019) as the most effective one is attending specific Cybersecurity training courses (71%), and the second one participating in professional organizations and events (68%), figure 4.

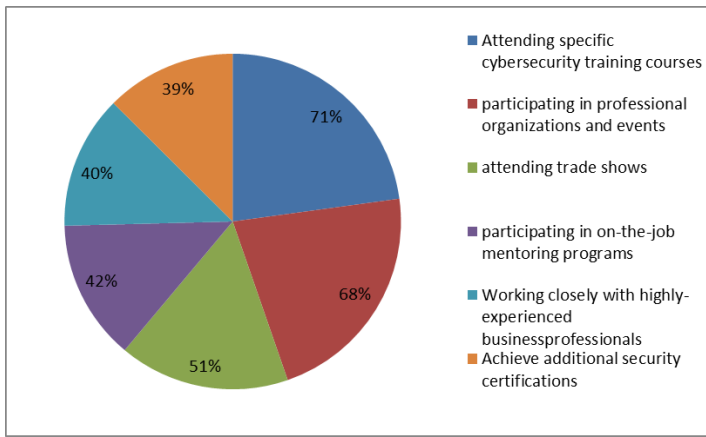


Figure 4. The most effective methods for improving knowledge and skills

The second option is to look for “cybersecurity expertise as a service” and outsource cybersecurity activities to MSSP (Managed Security Service Provider). The main reasons for outsourcing this function are (Rouse, 2018):

- Cybersecurity is becoming increasingly expensive
- It's far more cost effective
- Specialization is key for adequate protection
- MSSPs are important for demonstrating proper compliance with local and international standards
- A managed solution is one that is easy to scale
- MSSPs work around the clock and all over the world, so you know that your back is always covered.

The main question is how to select the adequate MSSP. The most important factor is its availability - 24x7 coverage of security operations. The suggestion is also to check its reputation and leadership, as well as supported systems and technologies. In addition to these, an important factor in selection process is the price. According to Cybersecurity Insiders (2019) the main drivers for using a managed service (MSSP) is ability to respond to incidents (48%) and lack of internal security personnel (48%), figure 5.

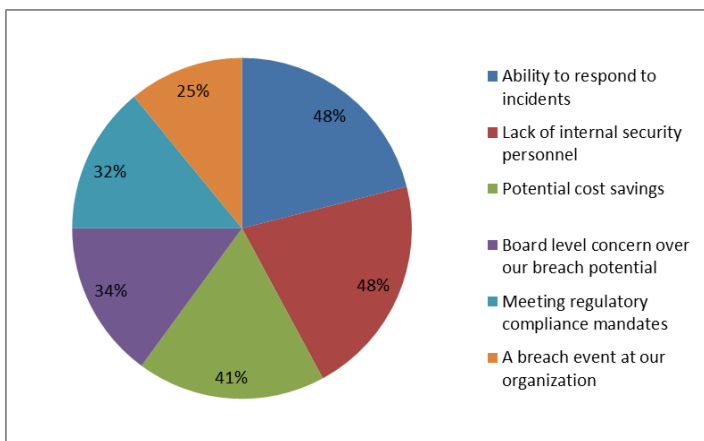


Figure 5. The main drivers for using MSSP

Also, it is possible to identify the third option. It is focusing to changing the hiring processes that should focus on candidates who are capable, enthusiastic and willing to learn, but without knowledge and certificates and learn them to take the responsibility and be up to date with novelties in this domain. Of course, this option is still very expensive like the first option, but it's easier to implement. There are not a lot of available cybersecurity experts so it is easier to find someone with the high education and willingness to learn. This option is good for entry-level security positions where security knowledge is not as critical. In this situation it is acceptable, maybe even better, to get someone with the right profile and train him or her on the job. Also as a potential Cybersecurity challenge, the informal processes of Cybersecurity were identified. To manage this challenge, it would be very useful to implement best practices for these processes according to the available international standards. One of them is ISO/IEC 27032 that considers digital assets, analyzes the risks over those assets and proposes security measures that can mitigate those risks.

Each organization contributes to the advancement of its cyber security by implementing the ISO/IEC 27032 standard, especially in the following areas:

- Information security,
- Network security,
- Internet security, and
- Critical information infrastructure protection (CIIP).

Which of the above options choose is the decision of each company. Also there are a lot of aspects of Cybersecurity that we can consider. One of them is high level of security program management. In this area the research (Cybersecurity Insiders, 2019) shows that majority of organizations confirm that their security programs are primarily operated in-house (53%). This is followed by over a third of organizations (38%) who operate in a hybrid fashion of in-house and outsourced resources or outsource all of their security operations. Also, for other aspect of Cybersecurity, related to endpoint security, most commonly the security issues are managed by an internal team (44%), but still less than managing security program. The internal experts are responsible for triage and remediation of security issues. Less than a third of organizations rely on a fully managed solution provided by an MSSP (27%), and 22% combine these two approaches.

Based on this research, we can conclude that companies still rely on their own resources, but obviously there is a trend of outsourcing some types of security jobs to more educated and experienced Security Service Providers. The very important reason for this trend is a large number of Cyberattacks, and the expected growth of the sophisticated attacks in the future. Therefore the small security teams in companies are not able to follow all novelties regarding new types of cyber-attacks and possible solutions. Probably the large companies will encourage strengthening their internal teams, but small and medium-sized companies will combine their own and external resources. In doing so, they are likely to retain management of security programs and policies, and outsource certain segments of technical security.

4. Conclusion

Regarding mentioned all these Cybersecurity threats and attacks we can see that the one of greatest threats that business faces today is Cybersecurity specialist and talent shortage. Based on different research studies and statistics we can summarize that Cybersecurity experts' shortage is very high, almost three million, and the expected knowledge and certificates of these experts are identified. The most important certificates are: CISSP, CISM, CompTIA Security+, CISA and CEH.

Organizations prefer to hire Cybersecurity experts from IT population because these experts already have some valuable knowledge about different types of technology and applications, networking and infrastructure, IT operations, IT support, programming, etc. Obviously, it is necessary to invest in education of the hired experts for adopting some new knowledge about Cybersecurity issues.

We can conclude that there are three possible solutions for solving a problem of Cybersecurity specialist and talent shortage. The first one is looking for the certified and experienced cybersecurity experts and keeping them well educated and trained during their employment. The second one is to look for "cybersecurity expertise as a service" and outsource cybersecurity activities to Managed Security Service Provider, and the last one is focusing to changing the hiring processes that should focus on candidates who are capable, enthusiastic and willing to learn, but without knowledge and certificates and learn them to take the responsibility and be up to date with novelties in this domain. The pros and cons of all of these options are explained in the paper.

5. References

Cybersecurity Insiders (2019): Managed Detection and Response Report, 2019.

Checkpoint: What is a Cyber Attack, <https://www.checkpoint.com/definitions/what-is-cyber-attack/>

Donegan, K. (2019): Lack of cybersecurity skills fuels workforce shortage, <https://searchsecurity.techtarget.com/feature/Lack-of-cybersecurity-skills-fuels-workforce-shortage>, published: August 2019.

Goud, N. (2017): Most Dangerous Cyber Security Threats of 2017, <https://www.cybersecurity-insiders.com/most-dangerous-cyber-security-threats-of-2017/>,

Goud, N. (2018): Most Dangerous Cyber Security Threats of 2018, <https://www.cybersecurity-insiders.com/most-dangerous-cyber-security-threats-of-2018/>,

Goud, N. (2019): 2019 Worst Cyber Attacks, <https://www.cybersecurity-insiders.com/2019-worst-cyber-attacks/>

Olsik, J. (2019): The Life and Times of Cybersecurity Professionals 2018, Research Report, The Enterprise Strategy Group, published: Apr 2019.

Richards, K. (2018): (ISC)2 Cybersecurity workforce shortage nears 3 million worldwide, <https://searchsecurity.techtarget.com/news/252450942/ISC2-Cybersecurity-workforce-shortage-nears-3-million-worldwide>, published: 19 Oct 2018.

Rouse, M. (2018): Managed security service provider (MSSP), <https://searchchannel.techtarget.com/definition/MSSP>, published: Apr 2018.

Top Cybersecurity Predictions for 2020 (31, December 2019): <https://resources.infosecinstitute.com/top-cybersecurity-predictions-for-2020/>

Copyright (c) 2022 Annals of Disaster Risk Sciences



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).