1st Bartosz Panek
Politechnika Opolska,
Wydział Elektrotechniki, Automatyki i Informatyki,
Opole, ul. Prószkowska 76
2nd Łukasz Patyk
Politechnika Opolska,
Wydział Elektrotechniki, Automatyki I Informatyki
Opole, ul. Prószkowska 76
3rd Przemysław Jura
Politechnika Opolska,
Wydział Elektrotechniki, Automatyki I Informatyki
Opole, ul. Prószkowska 76

Earnings in the data protection industry

KEYWORDS
Earnings, data protection, industry

ABSTRACT
Earnings for data protection specialists are becoming increasingly popular and important as more and more organisations realise the need to have specialists who are responsible for protecting their data. In this article we will discuss the earnings of data protection professionals, what qualifications and skills are needed to earn well in this field, and what the career and earnings prospects are for professionals in this field. We will also analyse the various factors that can affect the salary of data protection specialists, such as experience, industry and present data from the labour market.

I. INTRODUCTION

Cyber security and cryptography are some of the most important pillars of online security [1]. This is especially true at a time when technology development is at its fastest in years and people do not even know that they are using cryptography-based technologies in their daily lives [2]. It is evolving with newer and newer elements to improve security, but with this also comes better and better ways to break these security features. The very improvement in computer performance and the increase in the speed of calculations performed per second, e.g. by the creation of quantum computers in the future, will pose a serious challenge to our security and that of our data [2]. Already today we can see the problems faced by security people e.g. the declining ability of passwords to ensure the security of the IT system and beyond. One proposal to solve this problem could be the HSM(Hardware Security Module) as a basis for cryptographic key generation [3]. For the development of this solution, the authors looked, among other things, at information on secure key authentication using, for example, GDLP and IFP [4]. They also used ECG which provides secure key generation with relatively low latency [5].

The designed solution was compared with cryptographic frameworks that decouple keys from the application [6], this approach provided high functionality for all applications. Given that the usability of passwords as well as PINs is slowly coming to an end [7] an important aspect from a usability point of view will be the fact to reduce the number of passwords a person will have to remember. Therefore, the development of this field is very important for the market. Thanks to this, people who want to specialise in one of its branches should easily find the profession and the job they want [8]. The reason for this is that the development of technology and, therefore, the number of ways of securing sensitive data as well as breaches of security is constantly increasing, so new specialists will be needed to keep customers safe and companies will be forced to invest more and more in their own security [9].

II. RESEARCH

In order to create the charts that describe the information collected on specific Cyber Security sectors such as employment and salaries, for example, we used the website kaggle.com, which was the source of the data we used. The information there is presented in a clear and lucid manner. And, most importantly, they are the latest statistics from the

last three years. Then, this information we were interested in was collated together in 'Excel' and presented using column charts, as they make even the large number of records therein relatively easy to read, so that we can easily see the differences occurring between specific pillars of the values in question. Analysing the information contained in the database involved tracing in detail how the graphs behave for specific inputs in selected fields and categories. This enabled us to create accurate and detailed descriptions for each model. To make the graphs easier to understand, it is worth noting that the earnings shown are in dollars and the data used was itself obtained from an organisation located in the United States.

III. DISCUSSION

It's clear that the earnings of data protection professionals vary. These differences are graphically illustrated in Figure 1. In the chart, we see the distribution of the maximum annual payouts recorded for the data protection professions concerned. It can be seen that only nine professions in this sector exceed an annual income of one million, the rest rather fall below this rate. Such high salaries are due to the high responsibility of some professions and the fact that we consider maximum values. Rather, most professions take values between two hundred thousand and six hundred thousand.

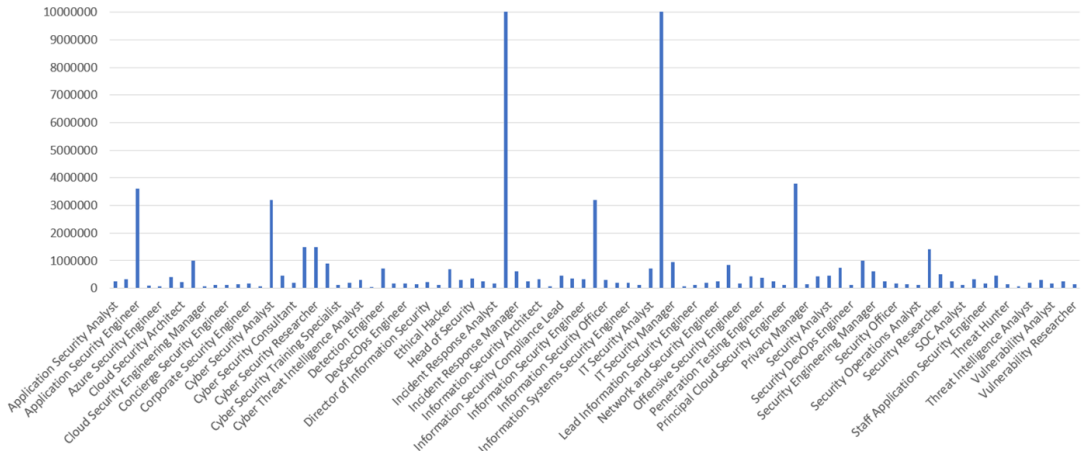

Figure 1. Maximum annual payments registered for the data protection professions concerned

In general terms, the earnings of data protection workers are shown in Figure 2. In the chart we can see the distribution of average annual payouts recorded for the data protection professions in question. Only four professions earn on average more than half a million per year, then there is another range for five professions that earn more than three hundred thousand per year and the rest earn rather below this three hundred thousand. A notable exception is the profession of "Incident Response Manager", which earns an average of one million a year.

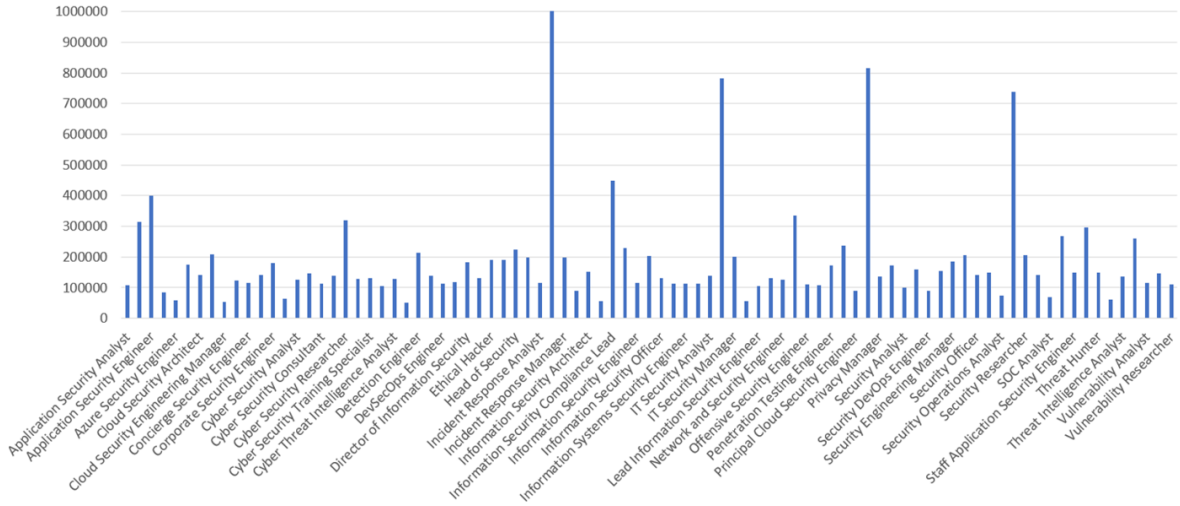

Figure 2. Average annual payouts recorded for the data protection professions

Unlike the previous charts, Figure 3 shows the minimum annual salary for data protection employees.In the chart we see the distribution of the minimum annual payouts recorded for the data protection professions concerned. The profession with the highest minimum annual salary is "Information Security Compliance Lead", followed by occupations such as "Application Security Engineer" and "Principal Cloud Security Engineer". The majority of employees in this case earn between fifty and one hundred and fifty thousand.

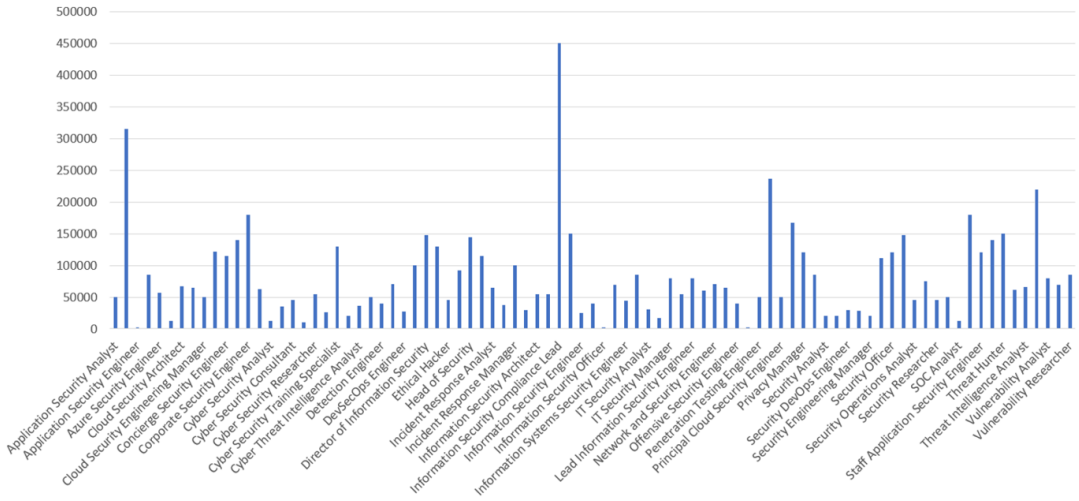

Figure 3. Minimum annual payments registered for the data protection professions concerned

The percentage share of individual professions in the data protection market is shown in Figure 4. In the chart, we see the percentage distribution by data protection profession. The most popular occupation is 'Security Engineer', with almost sixteen percent of data protection professionals working in this occupation. The next most distinguished occupation is "Cyber Security Analyst" with eleven per cent. There are only ten occupations with a significant percentage that make up the majority of the total.

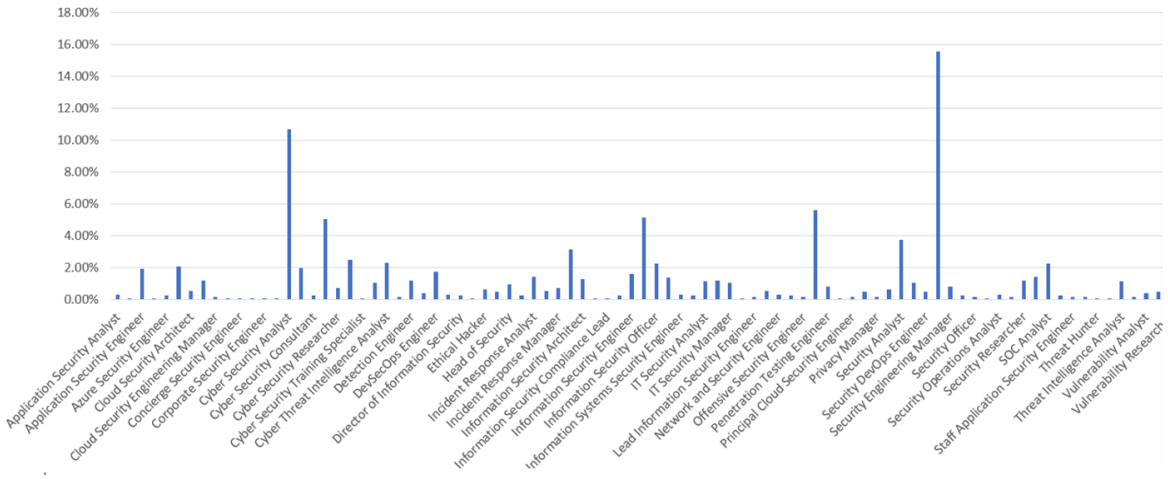

Figure 4. Percentage distribution of popularity of occupations in the data protection sector

The most popular data protection professions are shown in Figure 5. In the chart we see, the ten most popular occupations in the data protection sector. The most popular occupation is 'Security Engineer' with a significant lead over 'Cyber Security Analyst', with 'Penetration Tester' in third place. The least popular occupations are "Cyber Security Specialist", "Cyber Threat Intelligence Analyst", "Informaion Security Officer" and "SOC Analyst".

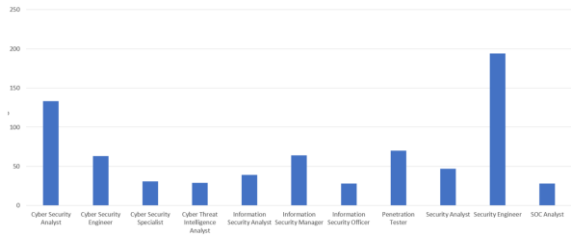

Figure 5. Top ten professions in the data protection sector

The distribution of annual earnings for the previously discussed most popular data protection professions is graphically presented in Figure 6. In the chart, we can see the distribution of the value of annual earnings recorded for the most popular data protection occupation. The largest number of workers, almost six percent, earn around one hundred and sixty thousand per year. The majority of employees in this profession earn between one hundred and twenty thousand and two hundred thousand per year. It is worth noting, that the lowest registered annual earnings are only twenty-eight thousand and the highest is three hundred thousand.

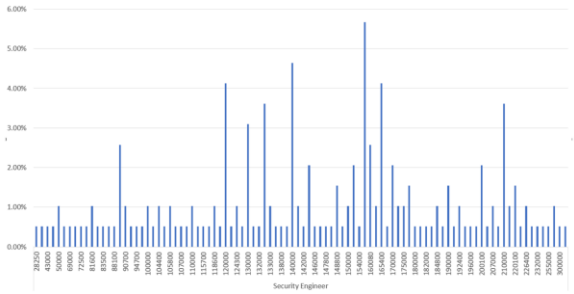

Figure 6. Distribution of annual earnings for the most popular occupation in the data protection sector

Of course, not all employees have the same education and professional experience. Therefore, the percentage distribution of employee experience in the data protection sector is shown in Figure 7. In the chart we see, the percentage distribution by experience in data protection. Experience has been divided into four levels: "Entry Level", "Middle Level", "Senior Level", "Expert". SE is the largest with almost half, followed by Mi with around thirty-three percent, and the smallest groups are the people with the most and least experience. The people with the most knowledge are the smallest, accounting for just five percent of the total.

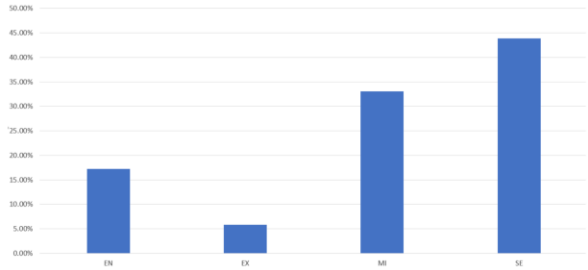

Figure 7. Percentage distribution of employee experience in the data protection sector

When considering the percentage distribution of employee experience by company size, Figure 8 should be analyzed. In the chart we can see the percentage distribution of employee experience by year and size of company in the data protection sector. What caught my eye is that for small and large companies the distribution of experience looks similar and there is a relatively similar number with each experience. It looks different in medium-sized companies where there are the least number of people with little experience.

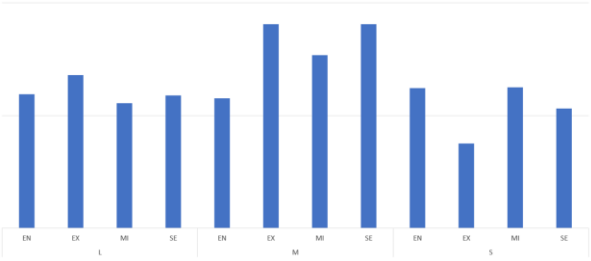

Figure 8. Percentage distribution of employee experience by company size in the data protection sector

Figure 9 shows that the percentage distribution of the size of companies in the data protection sector. The companies have been divided into three sizes: small, medium and large. The figures show that more than sixty per cent of the companies are large companies, followed by thirty percent of medium-sized companies and the smallest part of the market is made up of small companies, only around eight percent.

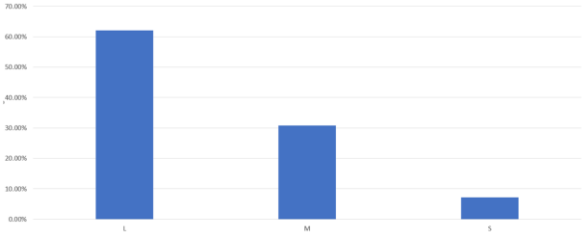

Figure 9. Percentage distribution of company size in the data protection sector

Figure 10 shows thepercentage distribution of the location of companies in the data protection sector. The United States dominates with seventy-one percent. Another twelve or so countries have a percentage higher than one or below, including the United Kingdom, Canada and Germany. This chart shows the role played by the United States in cyber security.

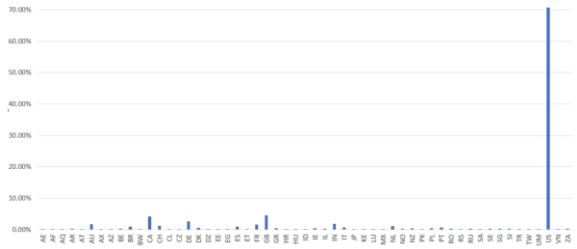

Figure 10. Percentage distribution of locations of companies in the data protection sector

In the Figure11 we can see, the percentage distribution of the origin of the employees in the data protection sector. This looks very similar to the graph with the company origin. The vast majority of registered employees work in the United States or in a company registered there, they represent almost seventy per cent of all employees. Only Canada, Germany and the United Kingdom still have more employees than the rest of the countries.

Figure 11. Percentage distribution of origin of data protection workers

In Figure 12, we can see the percentage distribution of origin and experience of employees in the data protection sector. The vast majority of registered employees work in the United States or in a company registered there, they account for almost seventy per cent of all employees. Of these, the majority are employees with SE or MI experience, there are far fewer EX-level employees as only about five percent.

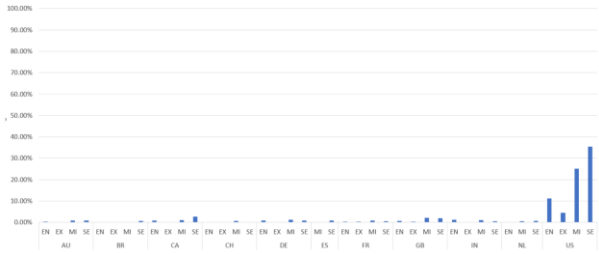

Figure 12. Percentage distribution of background and experience of employees in the data protection sector

IV. SUMMARY

Data protection professions are increasingly popular and important for the security of companies and institutions. The job of a data protection specialist involves securing and monitoring data against loss, theft or unauthorized access. It requires specialized knowledge and skills, as well as constant attention to new solutions and trends. In today's world, where data is one of the most important assets, data protection specialists are becoming essential for every organization. As a result, there are an increasing number of job vacancies on the market for specialists in this field. The requirements for candidates vary depending on the position, but a university degree, specialized certification or relevant work experience is usually required.

Data protection specialists are responsible for securing data from unauthorized access, monitoring data traffic, and responding to security incidents. The job also requires knowledge of data protection legislation, such as the RODO, and the ability to apply it in practice. This is very important as it not only protects data from unauthorized access, but also ensures its integrity and confidentiality. Data protection specialists are also responsible for creating and implementing data security policies, as well as training employees on data security. With the growing importance of data protection, professions in this field are increasingly in demand and appreciated. Data protection specialists can work in a variety of industries, such as banking, insurance, telecommunications or commerce. They may also work in the public sector or act as freelance professionals.

As technology is constantly evolving and regulations are changing, data protection specialists need to be constantly up to date with news and changes. This means that the job is dynamic and requires constant development and expansion of their competences.

In conclusion, data protection professions are an important and sought-after profession that involves securing and monitoring data against loss, theft or unauthorized access. It requires specialized knowledge, skills and continuous development. Data protection professionals are essential for any organization that wants to protect its data and ensure its integrity and confidentiality.

REFERENCES

[1] Devi.T, R.: *Importance of cryptography in network security*. Proceedings – 2013 International Conference on Communication Systems and Network Technologies, CSNT 2013, 2013, pp. 462–467. DOI: 10.1109/CSNT.2013.102.

[2] Bell, T., Thimbleby, H., Fellows, M., Witten, I., Koblitz, N., Powell, M.: (2003). *Explaining cryptographic systems*. Computers & Education, vol. 40(3), 2003, pp. 199–215, DOI: 10.1016/S0360-1315-(02)00102-1.

[3] Murtaza, M.H., Tahir, H., Tahir, S., Alizai, Z.A., Riaz, Q., Hussain, M.: (2022). *A portable hardware security module and cryptographic key generator*. Journal of Information Security and Applications, vol. 70, 2022, pp. 103332, DOI: 10.1016/J.JISA.2022.-103332.

[4] Meshram, C., Lee, C. C., Li, C. T., & Chen, C.L.: *A secure key authentication scheme for cryptosystems based on GDLP and IFP*. Soft Computing, vol. 21(24), 2017, pp. 7285–7291. DOI: 10.1007/S00500-016-2440-3.

[5] Rahimi Moosavi, S., Nigussie, E., Levorato, M., Virtanen, S., Isoaho, J.: *Low-Latency Approach for Secure ECG Feature Based Cryptographic Key Generation*. IEEE Access, vol. 6, 2017, pp. 428–442, DOI: 10.1109/ACCESS.2017.2766523.

[6] Mavrogiannopoulos, N., Trmač, M., & Preneel, B.: *A Linux kernel cryptographic framework: Decoupling cryptographic keys from applications*. Proceedings of the ACM Symposium on Applied Computing, 2012, pp. 1435–1442, DOI: 10.1145/2245276.-2232006.

[7] Stajano, F.: *Pico: No more passwords!* Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 7114 LNCS, 2011, pp. 49–81, DOI: 10.1007/978-3-642-25867-1_6/COVER.

[8] Pollmeier, S., Bongiovanni, I., Slapničar, S.: (2023). *Designing a financial quantification model for cyber risk: A case study in a bank*. Safety Science, vol. 159, 2023, pp. 106022, DOI: 10.1016/J.SSCI.2022.-106022.

[9] Fernandez De Arroyabe, I., Arranz, C.F.A., Arroyabe, M.F., Fernandez de Arroyabe, J.C.: (2023). *Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019*. Computers & Security, vol. 124,2023, pp. 102954. DOI: 10.1016/J.COSE.-2022.102954.