Past, Present, and Future of Cybersecurity for ICT-Professionals

Tommy Lin
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
t.z.lin@student.utwente.nl

ABSTRACT

As cybersecurity becomes more important, demand for skilled cybersecurity professionals keeps increasing. However, due to rapid changes in the field, a gap has formed between the skills people have when freshly done with their formal education, and the expectation of employers. That has led to surveys being done with cybersecurity professionals, to determine what they issues they have encountered when actually working. However, there has been very little analysis of occupational data, as opposed to surveys which is solely based on anecdotal experience. The aim of this paper is to start with literature research, to determine a suitable data set and data processing tools. Afterwards, quantitative data analysis will be done on occupational data to get an overview of the requirements regarding cybersecurity in ICT professionals. However, the used data set was not thorough and specific enough, and had some bias, allowing no decisive conclusions to be drawn.

Keywords

cybersecurity, professional, requirements, quantitative data analysis, O*NET

1. INTRODUCTION

Cybersecurity is a field that is becoming more and more important, as cyberattacks become more prevalent, and on a larger scale. For example, in 2020, the United States' Federal Bureau of Investigation (FBI) [7], received 791.790 complaints from individuals related to cyber crime . This amounts to an increase of 69% in complaints regarding internet crime compared to 2019, amounting to losses exceeding 4.1 billion USD.

Not only individuals are affected. Reports from Statista [15] show that in the United States of America (USA), the number of data breaches and amount of sensitive records exposed has seen an increase since 2005, with the past years all having over 1.000 data breaches in the USA alone. In the period of 2017 - 2020, every year over 100 million sensitive records were leaked. Statista [16] has also calculated the average cost of these breaches. This was calculated through lost revenue for the business, costs related to detecting the breach, costs associated with the escalation of the situation, and handling the aftermath, for example, monitoring (stolen) credit card data. These costs have been only increasing since 2013, with the current average cost being 8.64 million USD for a data breach in the USA.

To counter these growing threats, cybersecurity also has to improve. The security information market was forecast [3] to grow at an annual rate of 8.5 %, with the global information security market reaching a value of 170.4 billion USD by 2022 .

This in turn, leads to an enormous growth in demand for information security professionals. The USA's Bureau of Labor Statistics [2] projects a growth of 33% in demand for information security analysts . However, this rapid growth also leads to some issues. In many cases, due to rapid changes in the profession, which the education can not keep up with, there is a gap between expected skills and the skills in reality of a freshly graduated cybersecurity student [10].

From a report in 2014 [8], there are three main gaps in the transition from education to employment for cybersecurity. For the development of the growing cybersecurity market, these gaps should be rectified. They were identified as a competence gap, which is the difference in expected knowledge compared to what the applicants actually have. A professional experience gap, due to many applicants not having sufficient experience that companies expect. Lastly, an education-speed-to-market gap, where educational institutions can not adapt the material fast enough to keep up with the professional market. While the second gap requires a larger change in the education, the first and last gap can be addressed.

Addressing these gaps would be helpful for all professionals who have to deal with cybersecurity. This could not only be cybersecurity focused employees such as the Chief Information Security Officier (CISO), but also for example Database Architects, who can make sure that their data is safe.

To improve these gaps between expectations and reality, a clear overview of the actual current skill set of cybersecurity professionals is required. This way, educational institutions can tailor their curriculum better to the current cybersecurity threats professionals will have to deal with. This will lead to better prepared graduates, who are more suited for dealing with cybersecurity threats once they start working professionally.

While doing surveys with cybersecurity professionals is an option to gather data, quantitative analysis on occupational data can also be done, as this provides a more global overview. Occupational data also allows for comparing past and current data, which can be used to attempt to

36^{th} Twente Student Conference on IT Febr. 4^{th}, 2022, Enschede, The Netherlands.

find patterns which might hold for the future. Examples of institutions gathering occupational data are the U.S. Bureau of Labor Statistics [13] or the Employment Development Department of the State of California [5].

1.1 Research Goals

While occupational data might not give specific insights, the goal of this research is to determine global trends and an overview of expectations regarding cybersecurity, using occupational data. To formulate this more concretely, a SMART [1] research question has been made:

RQ: What are the current cybersecurity requirements for an ICT-professional, categorised per job, based on occupational data gathered over 6 weeks?

To answer the main question, it is best to divide it into smaller sub questions, to have clear and concise goals that can be finished more easily. Furthermore, there are some questions that can be answered through literature before starting the individual research. The following questions were determined to be necessary for answering the main research question:

RQ1: What is a suitable data set for this research?
A short literature search can be done to find a suitable and freely available occupational data set.

RQ2: What tools are necessary to process the data set into relevant data?
Due to the fact that occupational data will be researched, which is vast in volume, tools will be required to process this data efficiently.

RQ3: Which ICT-related job categories can be defined?
To limit the scope of this research, as only six weeks are available, this research will focus only on ICT-related jobs, as the expectation is that these jobs are the most likely to deal with cybersecurity.

RQ4: What different requirements can be defined from the data set?
The chosen data set will dictate what type of data will be available. Depending on the data set, this could be different types of requirements, for example, certifications and education, or the type of technology commonly used, or what kind of skills are useful.

2. RELATED WORK

Due to the increasing demand in cybersecurity from professionals, some research has already been done to determine what requirements are lacking in people trying to enter the cybersecurity field, or what skills are deemed important by current professionals. Currently, research related to this have been mostly based on surveys or analyzing job postings. It is useful to understand this, as it can provide insight into what data is important, and whether this research confirms such results. It can also help answer some of the sub questions, such as showing what data sets or tools are commonly used, or what common job categories are. Furthermore, it gives insight in how quantitative data analysis on occupational data might differ from current research.

A survey was done in 2020 with 48 cybersecurity professionals [1], to determine what cybersecurity professionals thought were the most important skills one should have before working in this field. This data was divided into three parts; knowledge, skills and abilities (KSA). While these varied depending on the exact specialization of cybersecurity for the interviewee, several KSA were common in all fields.

The most important aspects for knowledge were to remain up-to-date with events and changes in the field, to have an understanding of operating systems, to have knowledge of logic and logic structures, and to know how packet-analysis works. All of the important knowledge are identified as general knowledge, with more specific knowledge being less important.

This could also be seen in the important skills and abilities, which marked the most important soft skills to be collaborating, written communication and communication with clients, users and management to be highly important. None of the interviewed considered skill in a particular programming language important, again indicating that general skills are the most important for cybersecurity. The most important abilities were curiosity and adaptability, due to the field constantly changing and being up-to-date is very important for a cybersecurity professional.

A research in 2015 [12] also performed a research, but combined this with analysis of job postings. This research was solely focused on the Australian market, and the results found might not be correct for the current market, as the field of cybersecurity has seen massive changes in the past couple of years, as already mentioned. It does show however, that research techniques are not only limited to surveys to gather data about the requirements for cybersecurity.

This research found 33 unique job listings, by scanning advertisements on an Australian job site (Seek.com.au). These jobs were divided into 6 categories, Analyst, Consultant, Engineer, Security Assessor / Advisor, Manager, and Sales. Common requirements were then analysed for each category. While the hard skills differed depending on the specific category, all jobs valued soft skills highly. This was also found in their questionnaire, where it became important that professionals dealing with cybersecurity have to be good communicators and presenters, as they have to communicate and present their issues, ideas and findings often.

While no prior research has been done utilising occupational data to determine required cybersecurity skills for professionals, different types of research have been done using occupational data in an attempt to predict requirements for professionals.

An example is a research from 2003 [9], which uses the O*NET occupational data from the U.S. Bureau of Labor Statistics (BLS) to predict job requirements. This was done by applying a Job Component Validity (JCV) model, which is a model where the most important attributes for a job are analysed. This was done through testing jobs on the General Aptitude Test Battery (GATB), which is a cognitive test used by the U.S. Employment Services to determine correlations between job performance and cognitive abilities. Scores on this test were compared to O*NET Generalized Work Activities (GWA) data. Correlation coefficients between GATB test scores and GWA data ranged from 0.35 to 0.89. These coefficients were highest in jobs which required high cognitive abilities. This meant that O*NET data could potentially be used to create a database which facilitates employee selection, however, no further research could be found regarding this subject.

This research project will likely not be able to be as thorough as the prior mentioned research, due to the limited

[1] https://en.wikipedia.org/wiki/SMART_criteria

scope of the research project.

3. METHODOLOGY

This research can be divided into two main phases. An initial literature phase, during which **RQ1-RQ2** will be answered. These sub questions serve as background knowledge which will be necessary for the actual research phase. The second phase will be the research phase, in which **RQ3-RQ4** will be answered. This phase requires research in how the data set can be processed with the chosen tool from **RQ2**, to get results which show insight in how cybersecurity has changed for ICT-professionals.

To successfully answer **RQ1**, a literature search will be done regarding commonly used occupational data. During literature research for related work, it was already found that the U.S. BLS provides a large data set of occupational data. However, this is not the only occupational data set, and as such, more research should be done to determine what the most suitable data set is.

As for **RQ2**, literature research can be done to determine commonly used tools for quantitative data analysis. Because of the expected volume of data, manually researching this will likely not be possible. As such, a tool will be required to facilitate data processing. However, due to the time limitations on the research, it is best to choose a tool which is either easy to learn or a tool which is already familiar. According to a report from 2019 [14] from SlashData, Python is commonly used in Data Science, with over 69% of machine learning developers and data scientists using Python. Due to prior experience with Python, it is likely the tool to be used.

After completing the literature phase, the research phase can be started. **RQ3** should be answered to specify what the exact scope of the research will be. While some literature research can be done in common ICT job categories, it is dependant on the actual data set used, and which ICT related jobs they have within their data set. Within the data set, jobs related to ICT will be filtered through a full-text search.

Once the scope has been specified, the requirements can be researched. This will be dependant on the data set, but as mentioned in Section 2, prior research with O*NET data have shown that this data set includes general work activities, which can give insight in what kind of requirements are necessary for a job. The complete data set should be studied, to determine what parts of the data will be useful in determining requirements. This could include, but is not limited to, general work activities, education required, common skills, or tools commonly used.

4. DATASET

4.1 Choosing The Dataset

To determine a suitable data set, first research should be done in what occupational data sets are even available. To get a general overview, on the regular Google site, the search term "occupational data" was used. The regular site was used, as Google Scholar would also include data sets currently unavailable for the public. This resulted in the following list of general available occupational data sets.

As mentioned before, the U.S. Bureau of Labor Statistics (BLS) provides a database on occupational data, O*NET [2]. Due to its name, it is hard to get an accurate view of its use in research thus far, as searching "ONET" on Google Scholar does not result in the BLS data set, and searching for "O*NET" uses the asterisk wildcard in search engines, making the search results inaccurate. However, it has been shown that the usage of O*NET data can provide valuable insights, as mentioned in Section 2.

Furthermore, it provides both its current and a historical database, all of which is freely available. Each dataset has multiple files concerning different topics, such as "General Work Activities", "Education Training and Experience" or "Skills". Due to the size of these data sets, and the fact that past editions are also available, the O*NET data set would allow for a thorough research, where different subjects can be compared with past data.

As previously mentioned in Section 1, the Employment Development Department of California (EDD) [3] also provides occupational data. This data set however, does not provide any historical data, which is part of this research project, as it attempts to make a forecast based on past data. Furthermore, on the website of the EDD, it also references the O*NET data set, so the assumption is that for a more complete data set, the O*NET data is preferred.

The Organisation for Economic Co-operation and Development (OECD) [4] also provides data regarding skills used by adults, with data of roughly 250.000 adults. However, due to its grand scope, the actual data itself is very general and global. Data in this data set is concerned with skills such as national literacy and numeracy, national education level, adults under specific intelligence thresholds, etc. Due to this general nature, it is likely not suitable for this research, which is more specific towards cybersecurity in professionals.

Furthermore, there is also the possibility of contacting private companies that gather occupational data. In this case, Datarade [5] is a platform that allows you to contact companies which gather different types of data, such as occupational data. These companies can be found under "Job Postings Data". Contact was made with the companies "LinkUp Job Search Engine" and "Jobalytics", however, neither of these companies provided a free sample related to cybersecurity skills in professionals.

Due to these reasons, the choice was made to use the O*NET data set for this research, answering **RQ1**

4.2 O*NET Data

To get a better insight in what can be researched exactly, the entire data set was shortly studied to find out what each of the available files provided in terms of data, and how this data can be processed and utilised. After this, several files were chosen, which would be more likely to contain data that can be relevant. This was done due to the limited time, as ideally the entire data set would be analyzed.An overview of the most used files in this research, and a short description is shown in Table 1.

4.3 Processing the data

Because of the volume of data, it would be necessary to process and filter this data first, before an analysis could be done. During the methodology, it was hypothesised that Python would likely be the best tool to process the data, due to prior experience and widespread usage of Python in data science. Furthermore, utilising different Python packages, a single tool could be used to process, analyze and visualize the data. Python is also freely avail-

[2]https://www.onetonline.org

[3]https://www.labormarketinfo.edd.ca.gov/OccGuides/

[4]https://www.oecd.org/skills/

[5]https://datarade.ai

File Name	Description
Skills	All job titles are related to the same 35 skills, and given a score for both Importance and Level, denoting how important a skill is and what the expected level is. Due to the fact that all jobs are related to the same skills, the skills here are broad and general. For example: "Reading Comprehension"
Work Activites	All job titles are related to the same 41 different General Work Activities (GWA). They are also scored on both Importance and Level. Because all jobs are scored on the same skills, the skills are very general, for example: "Getting Information" is one of the GWAs.
Technology Skills	Examples of the technology used for each job is described in this file, along with a Commodity Title, to classify the kind of technology. The technology given is a broad example, for example, "Web Browser Software" is a technology, as opposed to naming a specific web browser.

Table 1. The files of the data set used and a short description

able, and sharing Python code facilitates others to reproduce this exact research. Furthermore, a literature research on Google Scholar, searching for the query ["data science" OR "data analysis" AND "tool" OR "program" OR "programming"], showed R and Python are widely used for data science or analysis. As there was no prior experience with R, this programming language was not preferred. Due to these reasons, Python was chosen, answering **RQ2**.

To process and analyze the data, several libraries were used. To read and manipulate the data, pandas [6] was used. To perform some mathematical functions, NumPy [7] is also necessary. Lastly, Matplotlib [8] is a useful library to visualize and present the data once it has been processed.

[6]https://pandas.pydata.org
[7]https://numpy.org
[8]https://matplotlib.org

To actually process the data, the data sets first had to be read. As O*NET keeps past editions of the data sets, and the aim is to compare current data with past data, data for the past 5 years was read. O*NET releases a new edition every quarter, however, as this research is more aimed at general trends, it was thought to be sufficient to read 1 data set per year.

To find out the job categories, the data was filtered. This was done by filtering the "Title" column as found in the files. Initially, this was done so that only titles containing (case insensitive) "cybersecurity","information security" or "cyber security" were included. This resulted in only 1 title, "Information Security Analyst". However, this 1 title represents multiple different jobs, as explained in the file "Alternate Titles". Examples of alternate titles include, "Computer Security Specialist", or "Information Systems Security Officer (ISSO)".

This would be the preliminary answer for **RQ3**, however, this would later be revised after discussion with the supervisor.

With the intended job category clear, the actual data could now be processed. The first step was to analyze the "Skills" and "Work Activities" files. It was assumed that these files would give the most insight in what is currently required in regards to the cybersecurity of a professional. The skills would showcase what type of skill set is required, whereas the work activities would show what a professional is required to do.

As explained in Table 1, these files contained a score for both Importance and Level. To account for this, as some skills might be very important, but require only a low level, or vice versa, it was assumed that these would have an equal weight. As such, when processing the data, these elements were sorted based on $Level * Importance$.

This processed data could then be visualized with Matplotlib, which is shown in Section 5.

However, there were some issues with this data. Firstly, the O*NET data does not update regularly, and as such, does not provide valuable insights in how the required skills or work activities have changed over time. In the case of both "Skills" and "Work Activities", it was updated only once in the researched time period. Furthermore, it became apparent that the data within these files was very general, and did not mention cybersecurity at all.

Because of this, the researched job categories was expanded, to determine if there were trends that could be found when comparing data between different job categories. To keep the data somewhat related, only other jobs within ICT were filtered. The case insensitive filter would now become:

"chief","security","cybersecurity","cyber security",
"information security","information technology",
"cyber","computer","database", or "network".

As this filter was quite general, it also allowed certain jobs to pass which were not related to ICT at all. To prevent this, the following terms would be excluded:

"guard","fire","except computer",
"transportation","clerks","tool",
"geographic","sustainability","teller","hardware".

This resulted in a list of 15 job titles, which can be seen in Table 2, resulting in a revised answer for **RQ3**.

However, the issue still remained that the "Skills" and

"Work Activities" files contained only very general data, and no data specific to cybersecurity. After looking through the data set again, it was found that the "Technology Skills" file could give insight in what kind of technology related to cyber security is used by these jobs. As this file does not contain any kind of scoring, the amount of technologies used compared to technologies related to cybersecurity were instead analysed. As the descriptions of the technologies used was standardized, this could be filtered through a regular text filter. This filter would pass only technology descriptions containing one or more of the following, case insensitive terms:

"security", "cybersecurity","cyber","virus", "protection","firewall", or "fire wall".

The resulting data would then be saved in a text format, to keep track of when security related technologies would be added or removed, and it would be visualized in a graph, separated per job category.

Title
Chief Executives
Computer and Information Systems Managers
Computer Systems Analysts
Information Security Analysts
Computer and Information Research Scientists
Computer Network Support Specialists
Computer User Support Specialists
Computer Network Architects
Database Administrators
Database Architects
Network and Computer Systems Administrators
Computer Programmers
Computer Systems Engineers/Architects
Information Technology Project Managers
Computer Science Teachers, Postsecondary

Table 2. Revised list of job categories related to ICT

5. RESULTS

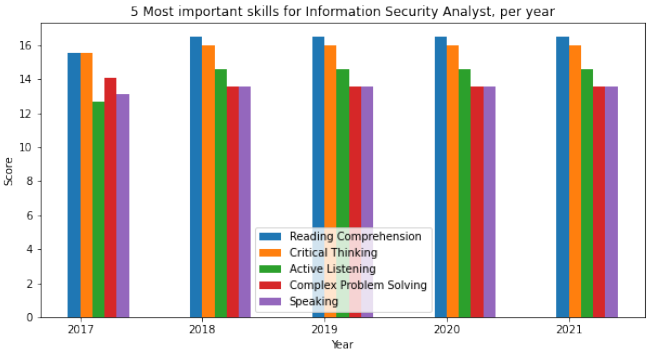

Figure 1. Annualized data of the most important skills for an Information Security Analyst

As mentioned in Section 4.3, it can be seen in both Figures 1 and 2 that the data regarding required skills and general work activities is only updated between 2017-2018 for an Information Security Analyst. For Figure 1, it can be seen that Reading Comprehension has always been and remained the most important skill, together with Critical Thinking. Active Listening became relatively more

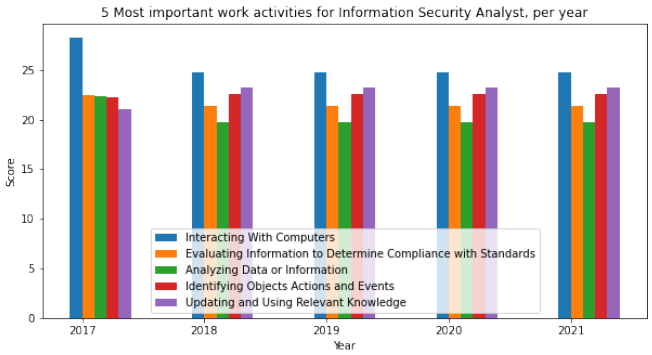

Figure 2. Annualized data of the most important activities for an Information Security Analyst

important, while Complex Problem Solving became relatively less important. Speaking always remained as the fifth most important skill. All of these skills are general soft skills, due to the fact that the data set only contains such skills, because all listed jobs were scored on the same skill set.

A similar pattern can be found in Figure 2, where all of the activities are general tasks. This is because all the Work Activities were also standardized, to score all types of different jobs on this standardized set of activities. The ranking does change over time however, with Interacting With Computers remaining constantly as the most important trait, but becoming relatively less important since the data was updated. Updating and Using Relevant Knowledge on the other hand, went from fifth most important to second most important. Evaluating Information and Analyzing Data or Information became relatively less important, going from second and third most important, to fourth and fifth respectively.

Table 3 shows the changes in technology used related to cyber security, as mentioned in the final part of Section 4.3. From this, it can be seen that there were relatively few changes; over 5 years, with 15 different job categories, only 11 changes happened, of which 6 were the same program, SolarWinds.

All of the data graphs documenting the changes in technologies used can be found in Appendix A, in Figures 7 - 36. Not all of these will be discussed, as many of these graphs show little to no change in the technologies used related to cybersecurity, or they follow a standard pattern which can be found for the majority of graphs for the overall technologies used.

In this data in the Appendix, it can be seen that almost all job categories, except for Information Security Analyst, Database Architects and Computer User Support Specialists had a sharp decline in number of technologies used between 2018-2019. Afterwards, these jobs would increase their amount of used technologies again, but the number still remained lower than 2018.

Furthermore, all job titles except for Computer Network Architects and Database Architects showed either no change in cybersecurity, or only one change, which was SolarWinds added in 2021.

For the Computer Network Architects, the only extra change besides SolarWinds was the removal of Firewall Equipment.

The data of technologies in general, and technology related

Job Title	Year	Change	Technology Name
Computer and Information Systems Managers	2021	Addition	SolarWinds
Computer User Support Specialists	2021	Addition	SolarWinds
Database Administrators	2021	Addition	SolarWinds
Network and Computer Systems Administrators	2021	Addition	SolarWinds
Computer Network Architects	2019	Removal	Firewall Equipment
Computer Network Architects	2021	Addition	SolarWinds
Database Architects	2019	Addition	Virtual Private Networking (VPN) software
Database Architects	2020	Addition	Database security software
Database Architects	2020	Addition	Encryption software
Database Architects	2020	Addition	McAfee
Database Architects	2021	Addition	SolarWinds

Table 3. All changes in cybersecurity related technologies per job title

to cybersecurity used by a Database Architect are explicitly shown in Figure 3 and 4, because this job category had the most significant changes in terms of technology used. For the Database Architect, the number of technologies related to cybersecurity was only 1 in 2017, and rose to 6 in 2021. The number of total technology used changed from 156 in 2017 to 317 in 2021.

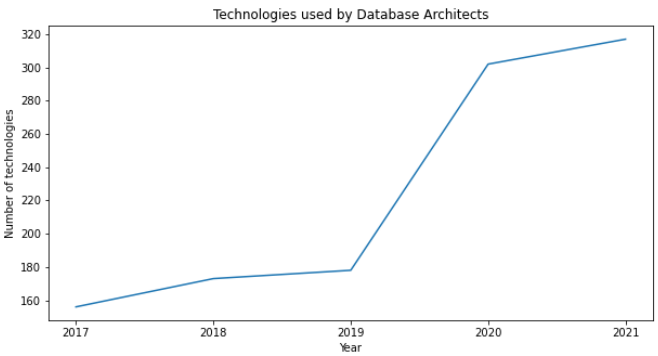

Figure 3. Annualized data of the amount of technologies used by Database Architects

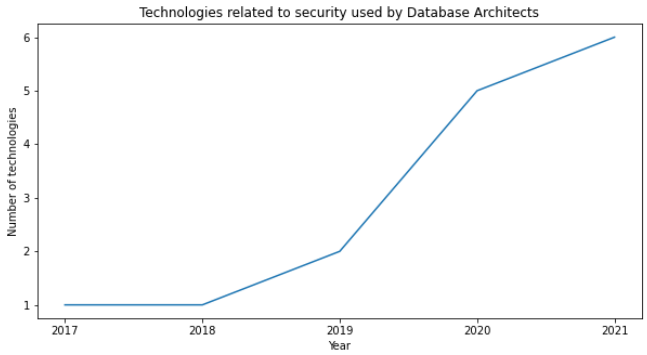

Figure 4. Annualized data of the amount of technologies related to cybersecurity used by Database Architects

The data of regular technologies used by a Computer User Support Specialist can be seen in figure 5, where it can be seen that the number of technology used has been rising every year, increasing from 171 in 2017 to 259 in 2021, resulting in a 51% growth in total technologies used. However, the amount of technologies related to cybersecurity only increased by one during this time period.

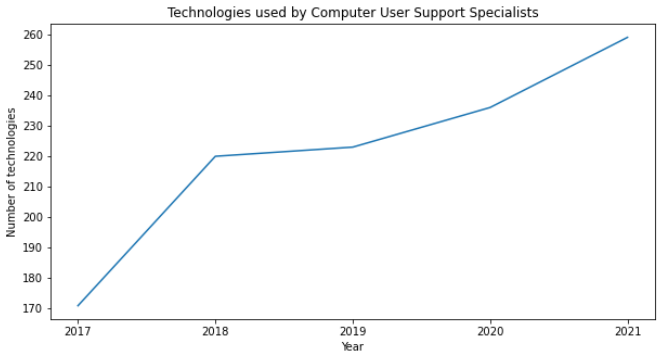

Figure 5. Annualized data of the amount of technologies used by Computer User Support Specialists

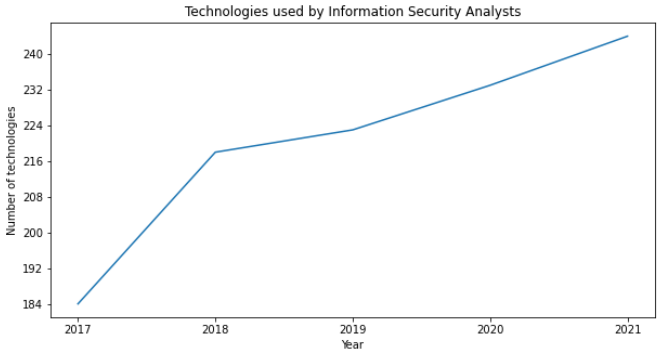

Figure 6. Annualized data of the amount of technologies used by Information Security Analysts

The last job category that did not see this decline in technologies used in 2018 was the Information Security Analyst. While the amount of technology did not change as significantly as with the prior two job categories, it still increased every year, going from 184 in 2017 to 244 in

2021. Furthermore, it did not see any changes related to the number of technologies used for cybersecurity.

6. CONCLUSION

This research attempted to document how the requirements of cybersecurity for ICT professionals have changed over the past five years, to try and find out how this could change in the future. This was done because the cybersecurity field is rapidly growing, and becoming more important than ever, as the amount of cyber attacks is also growing.

To facilitate the research, it was split into multiple smaller research questions. These questions would try to answer which data set would be best for this research, what tools should be used to process the data set, what different jobs can be defined from the data set, and how this data leads to the cybersecurity requirements for professionals. To answer the first two questions, literature search on Google Scholar was done. For the final two questions, data analysis on the O*NET data set was done.

The best data set for this research was determined to be the O*NET data set, from the U.S. Bureau of Labor Statistics. This was due to its free availability, volume of the data set, because its historical data is also available and it had prior usage in other related research.

To process this data set, Python was chosen. Python is commonly used by data scientists to process and research data, and due to its wide array of libraries, it can be suitable for different tasks. Furthermore, due to the limited time of the research, prior experience with Python was also a factor.

From the data set, initially only the "Information Security Analyst" job category was researched. This was due to the fact that initially, only jobs focussing on cybersecurity were researched. Due to the fact that this severely limited the data set, the filter was changed to include all ICT-related jobs in the data set. This would now include 15 job categories, as can be found in Figure 2. Researching this data set, it was found that the jobs within the data sets are general aggregated job categories, containing a lot of different specific jobs, which were all categorized under one job title. This is the reason there is only one job title focussing on cybersecurity specifically.

It is hard to draw a definitive conclusion for the last and overall research questions. This is because of the data relating to the change in skills and general work activities of the Information Security Analyst. During the researched five year time period of 2017-2021, there has only been one update to the data. However, with the available data, it does show that the general soft skills related to precise problem solving (reading comprehension, critical thinking, complex problem solving) and communication (active listening, speaking) were the most important before 2017, and have remained important until 2021. This seems in line with the literature mentioned in 2, where it was found that employees dealing with cybersecurity should be good communicators.

The data about the general work activities, which researched the same five year time period, was also only updated once. It is shown that keeping up to date with relevant knowledge has become more important, going from fifth most important to second most important activity. This result is similar to what was found in the literature in Section 2, in which a survey done with cybersecurity professionals answered that keeping up to date with events and changes in the field were of utmost importance.

However it is important to keep in mind that these conclusions are based off a five year time period during which only one update in the data set happened. To definitively confirm these conclusions, future work should be required. However, it is likely that this data was not updated regularly, due to the fact that the overall ranking of skills and work activities does not change much. This can also be seen within the results, as when it did update, the same five most important aspects stayed the most important, although the ranking within those five did change.

From the data related to technology used, SolarWinds was the most notable technology that got added during 2020-2021. This could be because of a large scale cyber attack [4], which happened during 2020, in which SolarWinds was heavily affected due to a leaked password. It is unlikely that due to this attack more employees started using SolarWinds. The more likely explanation is that due to this attack, the BLS would inquire more specifically towards the usage of SolarWinds, which would end up in the data of O*NET. This does also show that the O*NET data set is not completely unbiased. The data set favours technologies which have been part of large scale events, such as SolarWinds in this case. It is unlikely that only SolarWinds got added for all these jobs, however, due to the fact that this was part of a large event, it got specific attention for the data set. During this time period, much more smaller cybersecurity attacks happened, as mentioned in Section 1. However, the technologies related to these smaller events, do not get this kind of attention from O*NET.

Furthermore, for the data regarding regular technology used, it is hard to believe that twelve out of fifteen researched categories would suddenly use a significantly lower amount of technology after 2018. It is more likely that the BLS changed their data gathering with regards to technology during the period of 2017-2018. While the O*NET news site [11] does not go back far enough to see updates during 2017-2018, it does currently show that the dataset of February 2021 contains updated data for Technology Skills, to include data about distance learning and training, due to the COVID pandemic. As this shows that they do change the way they gather data about technology from time to time, it is possible that a similar situation happened for the 2018 data set.

For the removal of firewall equipment in 2019 for Computer Network Architects, it is likely that this was removed because it is redundant, as firewall software is still a tool shown in the current data.

The fact that Database Architects gained so many different technologies related to cyber security could be attributed to the fact that in general, the amount of technologies registered for a Database Architect increased significantly. It is also unlikely that this change reflects reality, as it is unlikely that the amount of different technologies used by a Database Architect doubled within five years. A more likely conclusion to draw is that more data was gathered by the BLS about technology used by Database Architects.

Furthermore, if the reported amount of technology related to cybersecurity does not change, it does not mean that the requirements for cybersecurity have not changed at all. While the amount of technology remains the same, it could be that the demands within a specific technology increases, raising the requirements within this technology.

Due to the fact that the data can not be conclusively used to determine what requirements changed, or for what reason, it is not possible to definitively answer **RQ4**, and as such, the main **RQ**. However, a lot of insight was gained into O*NET data, which could be useful for a future research.

7. LIMITATIONS IN THE RESEARCH

As mentioned in Section 6, there are several factors which limit the conclusions that can be drawn from this research. Firstly is the data set and the time limitations. As there was insufficient time to do both a survey and a regular research, a freely available data set had to be chosen. This resulted in less control in what the data set exactly should contain. Due to this, time had to be spent learning what exactly the data set contains, and how this is documented. Furthermore, the data set did not contain specific details which would have been useful in this research. In addition to that, for the data concerning the skills and general work activities, while a time period of five years was researched, the data set was only updated once in that time. While it could be argued that these factors do not change that much every year, and as such, new data does not need to be gathered every year.

Furthermore, as the data set was done by another party, the data set is dependant on their bias. It is unknown whether they kept their data gathering and data in general the same every year. In the results, it could be seen that there was a pattern between many jobs, where almost all of them followed the same trend line, where they reduced the number of technologies during 2018 - 2019. While a reason is given in Section 6, this reason is still dependant on the party gathering the data. Furthermore, in Section 6, it was mentioned that the likely reason SolarWinds has been added to several job categories, is due to the fact that this was part of a large scale cyberattack that year. However, as mentioned in Section 1, many smaller cyberattacks happen every year. However, these do not get reflected in the data. This shows that the data gathering is somewhat biased, as only large scale events will be shown in the data.

8. FUTURE WORK

As mentioned in Section 6, there are no definitive conclusions from the researched data set for the main research question. However, it does not mean that the data from this research can not be used at all. Firstly, it could serve as a reason for O*NET to start gathering more data specifically aimed at cyber security. Cyber security becomes more important as the internet becomes a more ingrained part of our regular and professional lives. A good understanding of cyber security is useful to any employee interacting with the internet.

Secondly, a short follow up to the possible conclusions posed in Section 6 could be done. In this section, there was uncertainty about why the data changed so drastically during 2017-2018. The most likely conclusion was that the way the data was gathered had changed. Contacting O*NET and asking these questions could resolve this.

Thirdly, the skill gap for cyber security professionals still exists. To address this, research is still required. A recommendation for such a research is that there should be a preliminary research, in which data is gathered through sources which are not O*NET. Currently O*NET data alone is not specific enough for such a research.

Lastly, O*NET data could still be useful for different types of research. As mentioned in Section 2, O*NET data can be used (when combined with other models) to determine large scale general trends. O*NET data could be used in tandem with different tests, such as the GATB, to determine a data base for requirements instead. From a literature search, it can be found that O*NET data becomes much more useful in conjunction with other data or models. Frey and Osborne [6] combined O*NET data with models based on Gaussian process classifiers to determine how susceptible specific job categories are to computerization.

9. REFERENCES

[1] M. E. Armstrong, K. S. Jones, A. S. Namin, and D. C. Newton. Knowledge, skills, and abilities for specialized curricula in cyber defense: Results from interviews with cyber professionals. Technical report, Federal Aviation Administration and Texas Tech University, 2020.

[2] Bureau of Labor Statistics. Fastest growing occupations, 2020.

[3] C. Canales, R. Contu, S. Deshpande, D. Gardner, E. Kim, and D. Kish. Forecast analysis: Information security, worldwide, 2q18 update, 2018.

[4] T. Claburn. We're not saying this is how solarwinds was backdoored, but its ftp password 'leaked on github in plaintext', 2020. [Online; accessed 21-01-2022].

[5] Employment Development Department of the State of California. Information security analysts, 2021. [Online; accessed 21-01-2022].

[6] C. B. Frey and M. Osborne. The future of employment: How susceptible are jobs to computerisation? Technical report, Oxford Martin Programme, 2013.

[7] Internet Crime Complaint Center. Internet crime report 2020. Technical report, Federal Bureau of Investigation, 2020.

[8] $(ISC)^2$. Cybersecurity workforce competencies: Preparing tomorrow's risk-ready professionals, 2014.

[9] P. R. Jeanneret and M. H. Strong. Linking o*net job analysis information to job requirements predictors: An o*net application. *Personnel Psychology*, 56:465–492, 2003.

[10] B. Lundell and J. Olstik. The life and times of cybersecurity professionals 2021 volume v. Technical report, ESG and ISSA, 2021.

[11] ONET. 'distance learning technology skills identified', 2021. [Online; accessed 21-01-2022].

[12] L. E. Potter and G. Vickers. What skills do you need to work in cyber security? a look at the australian market. In *SIGMIS-CPR '15: Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, pages 67–72, New York, NY, 2015. Association for Computing Machinery.

[13] relax U.S. Bureau of Labor Statistics. Information security analysts, 2021. [Online; accessed 21-01-2022].

[14] S. Shuermans and C. Voskoglou. The global developer population 2019. Technical report, SlashData, 2019.

[15] Statista. Annual number of data breaches and exposed records in the United States from 2005 to 2020, 2021. [Online; accessed 21-01-2022].

[16] Statista. Annual number of data breaches and exposed records in the United States from 2005 to 2020, 2021. [Online; accessed 21-01-2022].

APPENDIX

A. GRAPHS OF NUMBER OF TECHNOLOGIES AND TECHNOLOGIES RELATED TO SECURITY FOR EVERY RESEARCHED JOB

In this appendix section, all the results regarding the different technologies and different technologies related to cybersecurity used by different job categories in the ICT-field are shown. As many jobs follow a similar pattern for normal technologies, or have little to no change in the technologies related to cybersecurity, these are not discussed in the Results section.

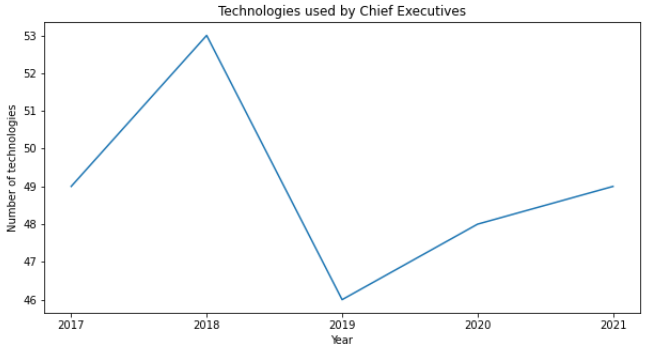

Figure 7. Annualized data of the amount of technologies used by Chief Executives

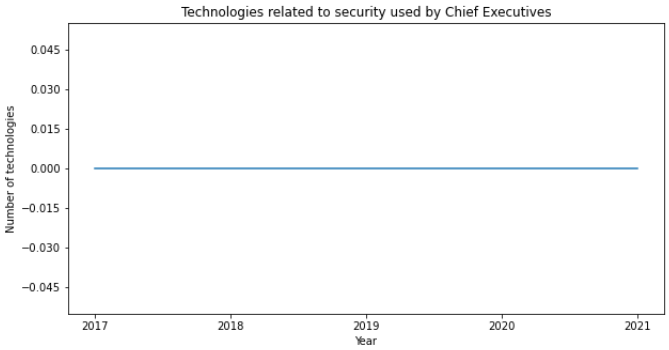

Figure 8. Annualized data of the amount of technologies related to cybersecurity used by Chief Executives

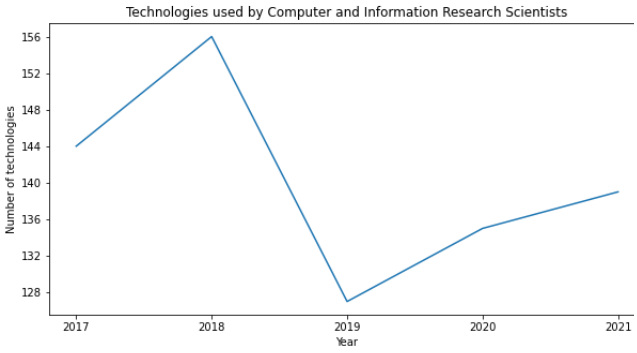

Figure 9. Annualized data of the amount of technologies used by Computer and Information Research Scientists

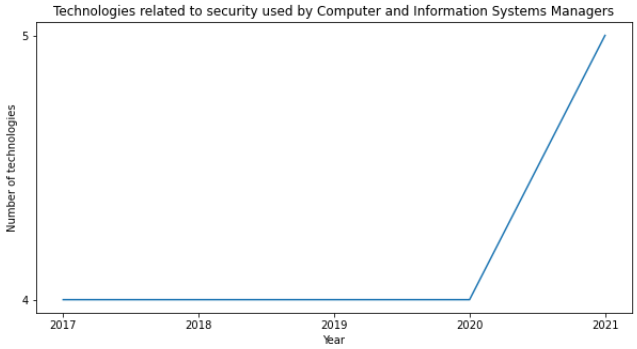

Figure 12. Annualized data of the amount of technologies related to cybersecurity used by Computer and Information Systems Managers

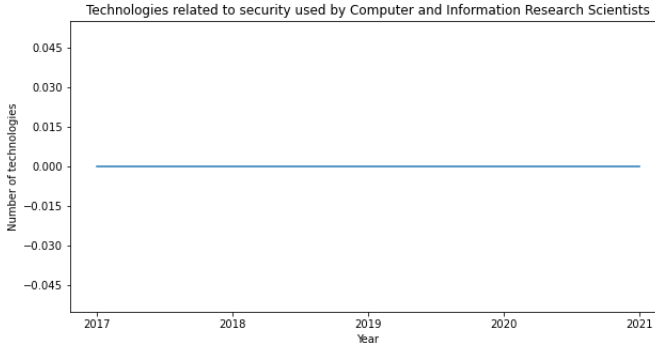

Figure 10. Annualized data of the amount of technologies related to cybersecurity used by Computer and Information Research Scientists

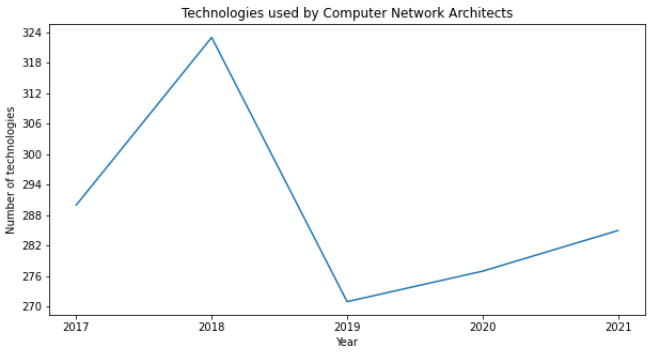

Figure 13. Annualized data of the amount of technologies used by Computer Network Architects

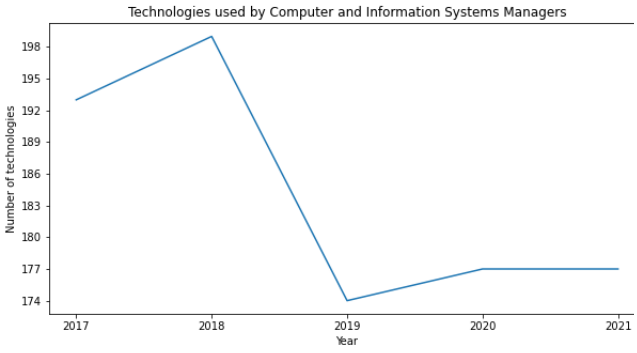

Figure 11. Annualized data of the amount of technologies used by Computer and Information Systems Managers

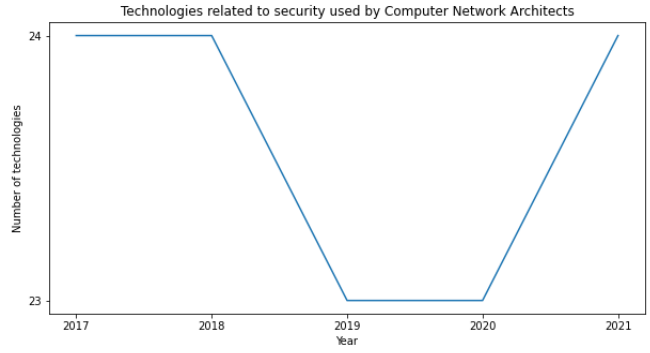

Figure 14. Annualized data of the amount of technologies related to cybersecurity used by Computer Network Architects

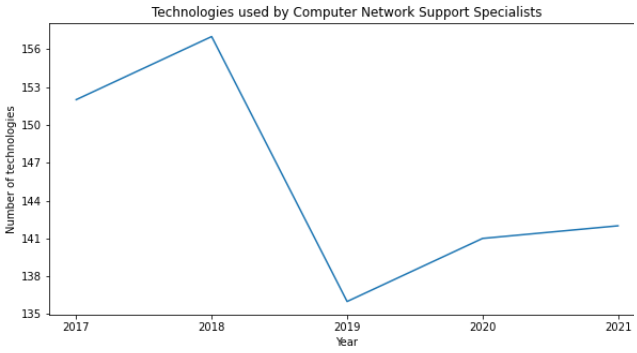

Figure 15. Annualized data of the amount of technologies used by Computer Network Support Specialists

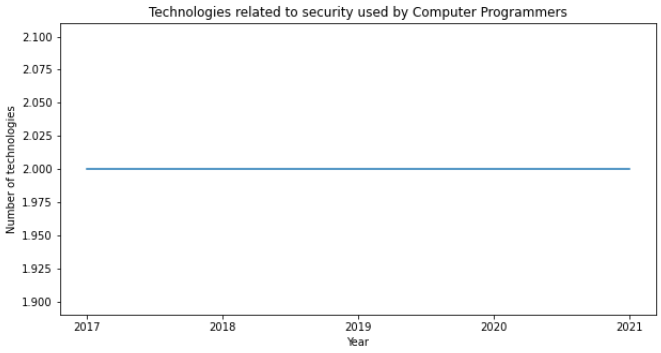

Figure 18. Annualized data of the amount of technologies related to cybersecurity used by Computer Programmers

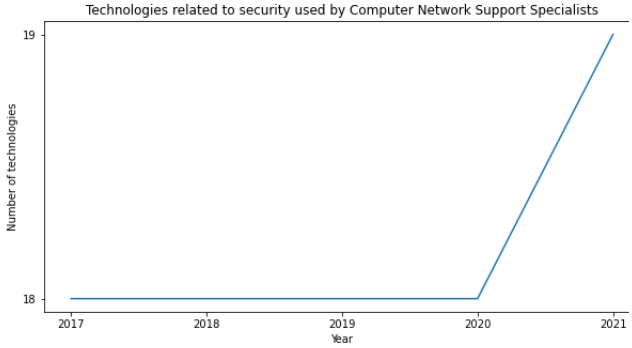

Figure 16. Annualized data of the amount of technologies related to cybersecurity used by Computer Support Specialists

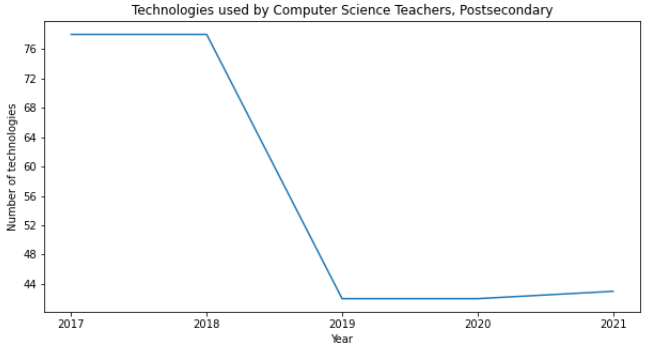

Figure 19. Annualized data of the amount of technologies used by Computer Science Teachers

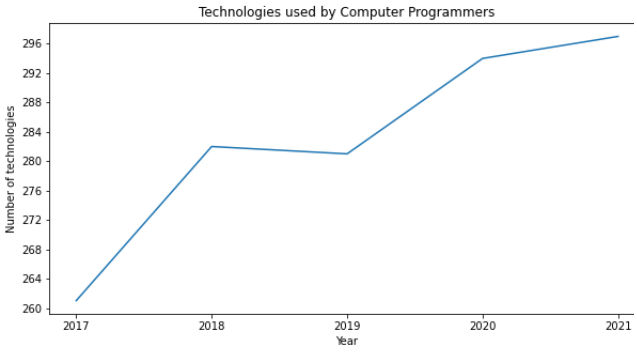

Figure 17. Annualized data of the amount of technologies used by Computer Programmers

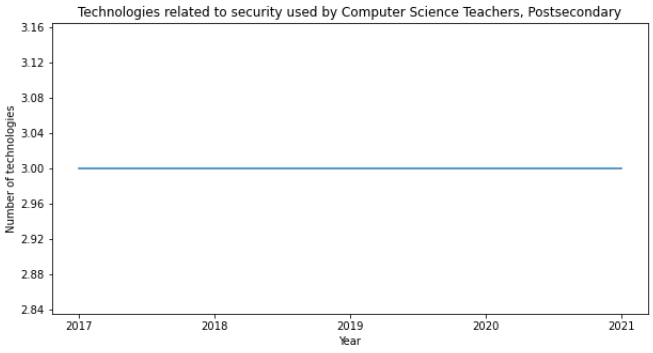

Figure 20. Annualized data of the amount of technologies related to cybersecurity used by Computer Science Teachers

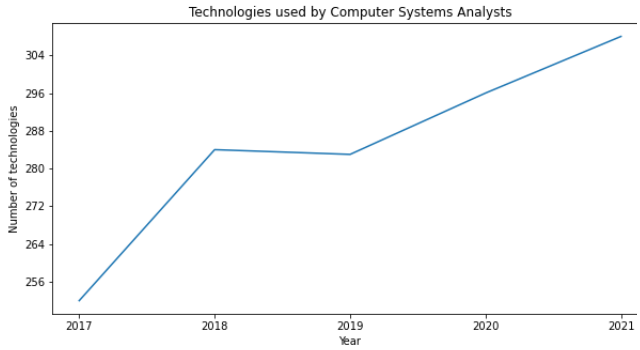

Figure 21. Annualized data of the amount of technologies used by Computer Systems Analysts

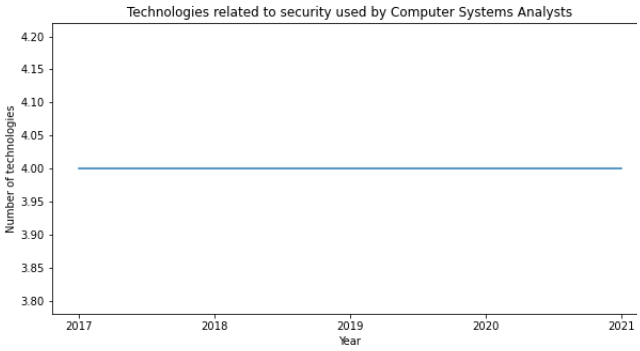

Figure 22. Annualized data of the amount of technologies related to cybersecurity used by Computer Systems Analysts

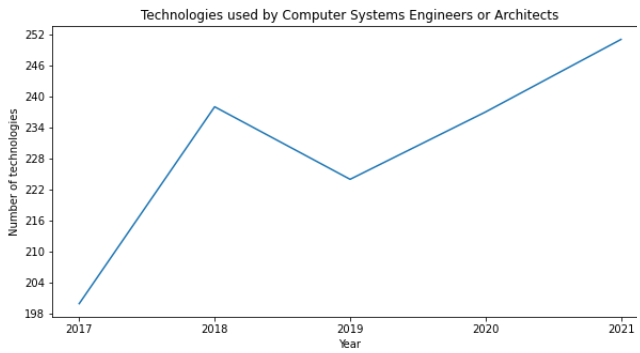

Figure 23. Annualized data of the amount of technologies used by Computer Systems Engineers

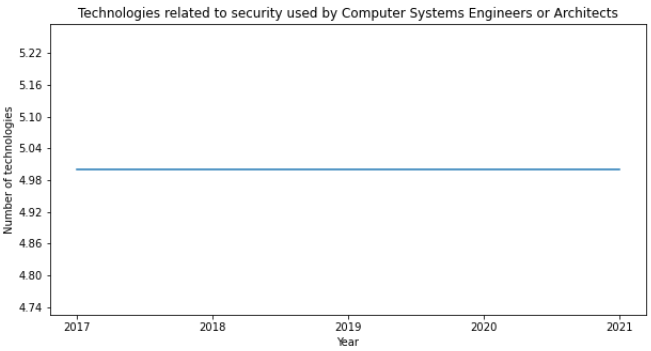

Figure 24. Annualized data of the amount of technologies related to cybersecurity used by Computer Systems Engineers

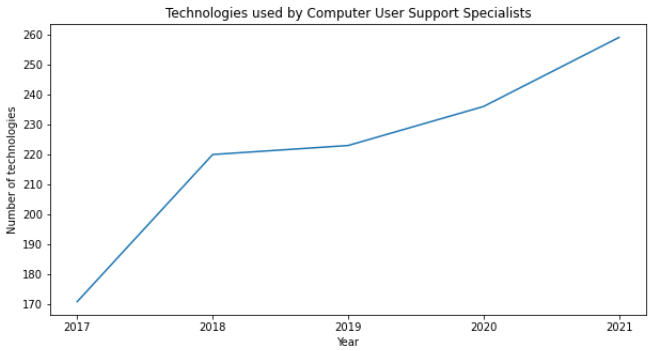

Figure 25. Annualized data of the amount of technologies used by Computer User Support Specialists

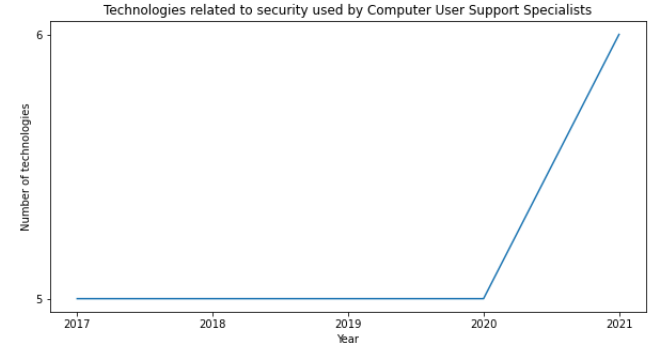

Figure 26. Annualized data of the amount of technologies related to cybersecurity used by Computer User Support Specialists

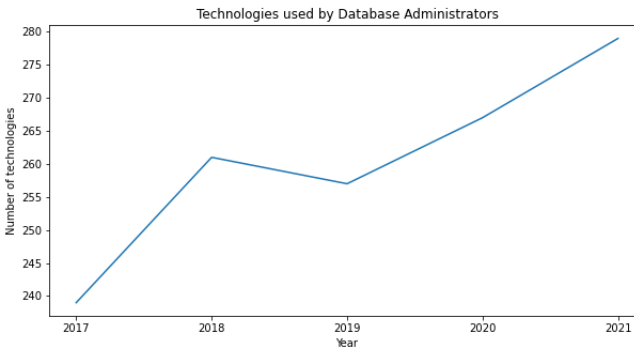

Figure 27. Annualized data of the amount of technologies used by Database Administrators

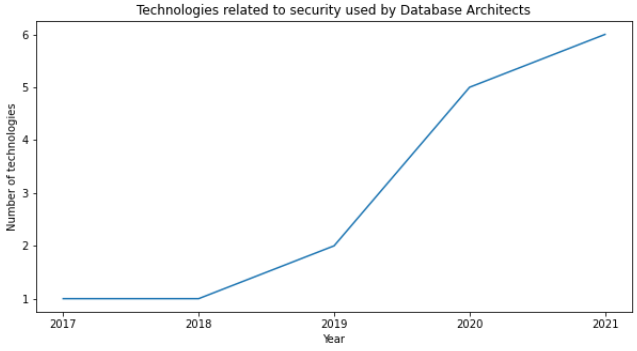

Figure 30. Annualized data of the amount of technologies related to cybersecurity used by Database Architects

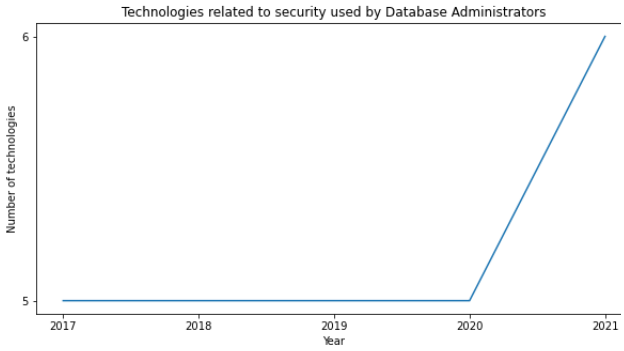

Figure 28. Annualized data of the amount of technologies related to cybersecurity used by Database Administrators

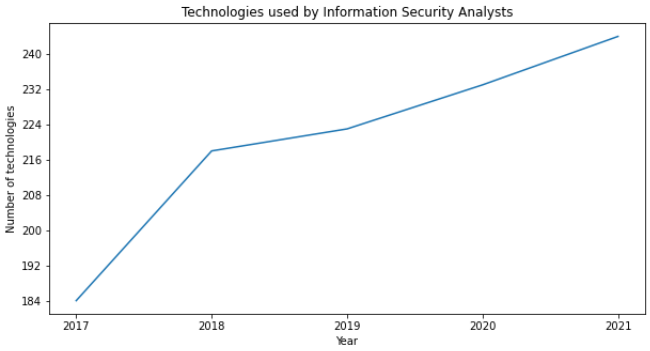

Figure 31. Annualized data of the amount of technologies used by Information Security Analysts

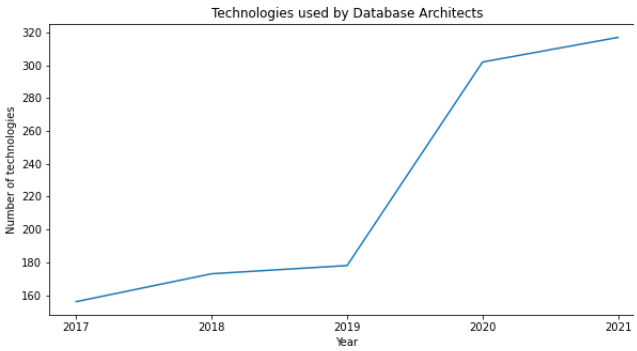

Figure 29. Annualized data of the amount of technologies used by Database Architects

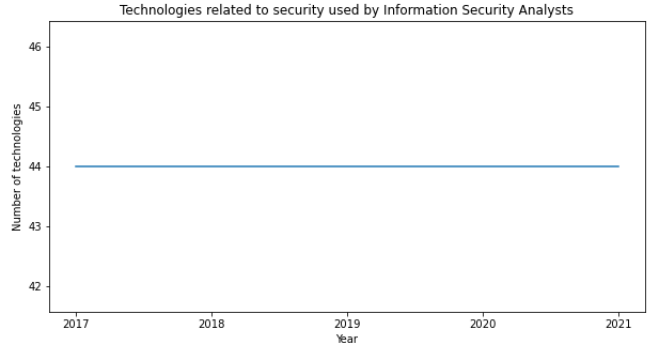

Figure 32. Annualized data of the amount of technologies related to cybersecurity used by Information Security Analysts

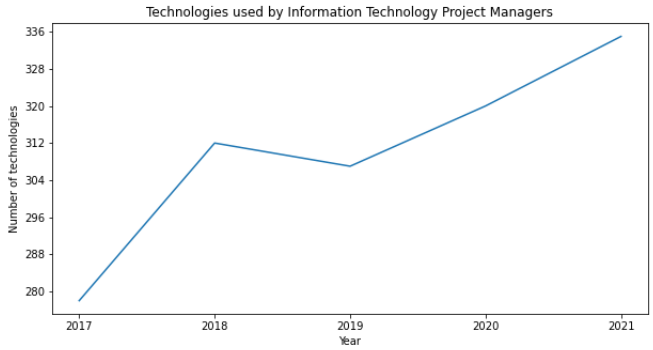

Figure 33. Annualized data of the amount of technologies used by Information Technology Project Managers

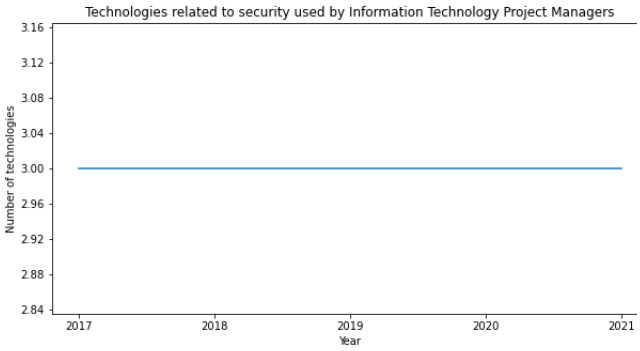

Figure 34. Annualized data of the amount of technologies related to cybersecurity used by Information Technology Project Managers

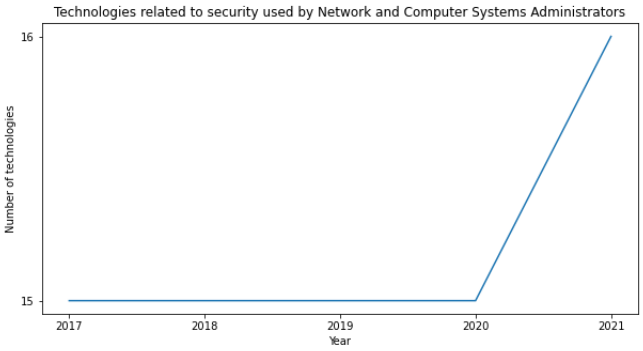

Figure 36. Annualized data of the amount of technologies related to cybersecurity used by Network and Computer Systems Administrators

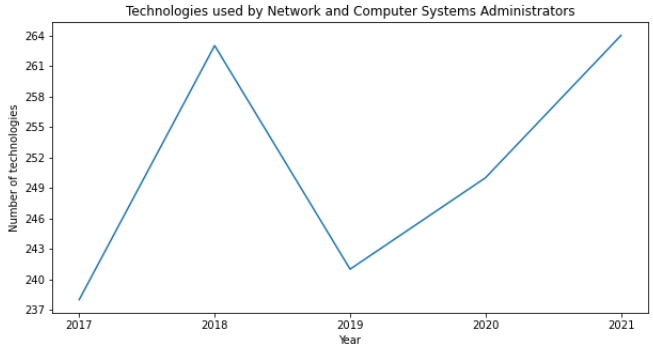

Figure 35. Annualized data of the amount of technologies used by Network and Computer Systems Administrators