Cyber Range as a Competency Based Education Instrument in Cyber Security

Ionuț Lateș[1] and Cătălin Boja[2]
[1)2)] *Bucharest University of Economic Studies, Bucharest, Romania*
E-mail: ionut.lates@csie.ase.ro; E-mail: catalin.boja@ie.ase.ro

Please cite this paper as:

Lateș, I. and Boja, C., 2022. Cyber Range as a Competency Based Education Instrument in Cyber Security In: R. Pamfilie, V. Dinu, C. Vasiliu, D. Pleșea, L. Tăchiciu eds. 2022. *8th BASIQ International Conference on New Trends in Sustainable Business and Consumption.* Graz, Austria, 25-27 May 2022. Bucharest: ASE, pp.703-710.

DOI: 10.24818/BASIQ/2022/08/093

Abstract

The importance of Cyber Security is becoming more and more widely known among companies and government institutions. This came at a cost that many business and public administration entities have paid in recent years. This indirect cost is due to the multitude of cyberattacks to which they have been subjected, attacks directed to the IT infrastructures of these entities. Recent studies show that most cyberattacks were based on vulnerabilities caused by the human factor: either directly, through the mishandling of technology (hardware and software), or indirectly, through the misconfiguration of cyber services exposed on the Internet. Cyber Range systems can offer multiple functionalities depending on the field of activity for which they are implemented. One of the main advantages of Cyber Ranges is that these systems can make a major contribution to the digitization of educational platforms, regardless of the field of study. This study aims to contribute to the process of educational environment optimization by addressing the influence of implementing Cyber Range systems as part of the digitalization of the educational process, particularly in the sphere of cybersecurity training. The conclusions presented in this article might have a major positive influence on educational effectiveness if they are implemented. The immediate impact in the field of cybersecurity is a financial one, as trained users reduce the risk of costly cyberattacks.

Keywords

Cyber Range, Cyber Security Awareness, Educational Cyber Instruments, Competency-based-Education.

DOI: 10.24818/BASIQ/2022/08/093

Introduction

According to recent studies performed by many companies from the cybersecurity field, human factors are responsible for approximately 95% of the data leaks through cyberattacks. Even if there are many implications of the human factor regarding cyberattacks vectors, two main types of human errors can be mentioned, from the cybersecurity breach vectors: IT systems misconfiguration and users misleading, convincing users to perform malicious actions without them being aware of the consequences (IBM, 2021). While lowering the chances of error is critical, there must also be considered the causes of error from a human perspective. Educating company/government institution staff about security fundamentals and best practices allows them to make smarter decisions, keep security in mind, and seek more guidance when they're unsure of the ramifications of a certain action. Employees should be trained on all core security issues (US Bureau of Labor Statistics, 2022). Because human error can manifest in a variety of ways, it's critical to provide employees with a basic understanding of any security topics they might encounter in their day-to-day work activities. Email, the internet, and social media, as well as phishing and malware training, are all issues that should be covered throughout training (Columbus, 2020).

For an employee who has access to a secure computer, training must be engaging and relevant: your employees have short attention spans, and you must guarantee that their training does not put them to sleep. Image and video-based interactive training courses are considerably more successful than hour-long PowerPoint sessions. Training should also not be delivered in yearly sessions that your employees will

forget a week later, but rather should be delivered in a quick and simply digestible format on a regular basis throughout their working lives (Pham, et al., 2016).

Cyber ranges are complex IT systems used in different activity fields. They consist of multiple modules being able to offer network infrastructures as a service (IaaS) combined with specialized software responsible for the customization of the system according to the activity field implementing it. From the cybersecurity perspective, cyber range systems can make a significant contribution to cyber security training ensuring cyber security virtual scenarios development. Cyber ranges are used in cybersecurity training to allow learners to obtain practical experience through hands-on activities. This type of activity will certainly increase the level of user training and cyber security awareness, thus reducing the risks of successful cyberattacks.

1. Research methodology

The research was conducted in phases and was based on the major processes in scientific investigation:

i. Formulation of the hypothesis: Cyber Range systems as a competency-based education instrument in the cyber security field;
ii. Conducting a specialized bibliographic study in the field;
iii. Conducting a study on statistics on recent years cyber security incidents; Analysis of human causes - employees and cyber security experts;
iv. Elaboration and development of arguments regarding the working hypothesis;
v. Formulation of conclusions and future work elements.

2.. Literature review

Cyber range systems are already successfully used as a competency-based education instrument in the cyber security field. There are many implementations of cyber ranges in large companies or government institutions of some states. There are also businesses implemented based on cyber security training through cyber range systems (Offensive Security, EcCouncil, Hack the box, etc.).

There are numerous cybersecurity courses available now for both beginners and advanced learners. The major goal of the courses for beginners is to increase their knowledge of cyber threats and to assist them develop their skills in safeguarding themselves and their businesses. Advanced courses, on the other hand, concentrate on profound security topics (European Cyber Security Organisation (ECSO), 2020). Most of the curriculum necessitates trainees dealing with difficult and hands-on experience with real-life events. A cyber range is a virtual world that participants can access and study during training to find answers to questions and learn practical skills. It is specifically built for a training session, as it includes all the infrastructure (machines, networks, tools, and so on) as well as security settings connected to the course's content. It must also be well-controlled from the standpoint of networking, which must be isolated from the outside to prevent traffic leakage and divided among trainees to prevent access to each other's environment. Currently, preparing cyber ranges for cybersecurity training is done manually, which is time consuming, requires a great deal of effort and talent, and is prone to errors (Pham, et al., 2016; European Cyber Security Organisation (ECSO), 2020).

It's worth noting that human mistake is to blame for 95% of data breaches. Businesses may address this growing tendency in data breaches by focusing on effective cybersecurity training for the company's personnel - increasing the awareness level and decreasing the risks (Irwin, 2022).

Education is changing continuously by trying to adapt to technology, demographic trends, and social changes. Human society is in a continuous change and that affects the way we learn or the expectations of others on the results of these processes. Last years, especially the unexpected embrace of online learning and other online communication technologies in the light of the COVID-19 pandemic, has again shift the focus of the society on the required changes that must be made in education. Despite it is not a new concept, Competency-based Education it has seen a surge of interest in recent years, based on its core philosophy, that education must focus on what students know and what practical skills they have, rather than how long they need to acquire the knowledge (Klein-Collins, 2016). For technical fields like computer science this approach has been proven to deliver better results as the main objective is to train the student to be able to do something (Dieck-Assad, Ávila-Ortega and González Peña, 2021; Malonda, 2022).

3. Cybersecurity recent years statistics

Not only has the number of exposed records from data breaches increased in 2020, but so has the number of phishing and malware attacks. Over 27 billion records were revealed in the first half of the year, vastly outnumbering the total amount of records disclosed in the entire year by 12 billion. These data breaches impacted a wide range of companies, including the hotel and technology industries. For example, in March 2020, 5.2 million guests of the hotel chain Marriott had their data breached by hackers. Marriott's internal data system, which contained contact information, names, and addresses, was targeted by the hackers. Hackers targeted Zoom, a video conferencing service that has grown in popularity because of the pandemic, in April. On dark web forums, over 500,000 Zoom account credentials were offered for purchase (Purplesec, 2021).

The situation imposed by the covid-19 pandemic has led to the implementation of the work-from-home concept for numerous companies in all fields of activity. This factor has involved an artificial acceleration of the development / reconfiguration of IT infrastructures so that IT services can be available both on-site and remotely. Given the fact that this transition process, from work at the company headquarters to remote work, was carried out in a short time and without a consistent training of staff (from the perspective of cyber security and not only) an increase was identified to successfully block cyberattacks that cause data leaks.

Training should be employed as a crucial risk reduction in the fight against cybercrime. To tackle the threat of cyberattacks, cybersecurity training is the best option. Cyber dangers can be considered and blocked before they develop using cybersecurity training for personnel. COVID-19 changed not only how people work and communicate with one another, but it's also causing a surge in cybercrime. Upskilling and reskilling are being addressed as continuous cybersecurity professional training is critical and the most effective method of combating cybercrime (Purplesec, 2021).

According to the research report publicly revealed by IBM research division, the average total cost of healthcare grew by 29.5 percent from $7.13 million in 2020 to $9.23 million in 2021. Energy went from second to fifth place in terms of cost, dropping from $6.39 million in 2020 to $4.65 million in 2021. (27.2 percent decrease). Services (7.8% increase), communications (20.3% increase), consumer (42.9 percent increase), retail (62.7 percent increase), media (92.1 percent increase), hospitality (76.2 percent increase), and the public sector (76.2 percent increase) were among the other industries that saw significant cost increases (78.7 percent increase). The top five industries for average total cost were: healthcare, financial, pharmaceuticals, technology and energy (IBM, 2021).

Another IBM research results reveal that the compromised credentials were the most common first attack vector in 2021, accounting for 20% of all breaches. Next, the entire range of the attack vectors and the impact regarding the costs associated with the data breach are presented.

In 2021, the most common initial attack vectors were (1) compromised credentials, which accounted for 20% of breaches, (2) phishing, which accounted for 17% of breaches, and (3) cloud misconfiguration, which accounted for 15% of breaches. Only 4% of breaches were caused by business email compromise, yet the average total cost of $5.01 million was the highest. Phishing ($4.65 million) was the second most expensive first attack vector, followed by malicious insiders ($4.61 million), social engineering ($4.47 million), and compromised credentials ($4.37 million). In 2021, the top four first assault vectors were the same as in 2020, however they were significantly re-ordered. Phishing has risen from fourth to second place, while cloud misconfiguration has dropped from second to third place. Figure 2 graphically illustrates the attack vectors impact from the data breaches cost perspective:

Figure no. 2. Data breach costs by cyber attack vectors - IBM 2021 data breach statistics

Source (IBM, 2021)

The conclusion made according to these results is that human factor is responsible for 6 out of 10 attack vectors, as it follows (Purplesec, 2021):

● *Social engineering, phishing and compromised credentials*: all these three categories represent attack vectors based on the lack of awareness of the situations in which an attacker uses social engineering means to obtain confidential information; recognizing and dealing with these situations is particularly important and can only be achieved by educating / training the employees - users of the IT infrastructure;

● *Business email compromise:* the prevention of such situations can be achieved by training the staff in such a way as to comply with the security procedures regarding accessing and handling the work email,

● *Accidental data loss/lost device:* even if the data/device is accidentally lost, the information cannot be disclosed if proper cryptographic mechanisms are implemented and data protection procedures are followed;

● *Cloud/IT infrastructure misconfiguration:* cybersecurity training should be part of the network infrastructure administration specialists' curricula; internet exposed services configuration need to be performed taking into account the exposure to cyber security risks.

Training staff to be aware of cyberattacks is a lengthy procedure. It is very important that the training process is largely based on practical, concrete, real-world situations - the environment in which they work daily. By simulating situations in which their actions play an important role in preventing a cyber-attack, they will be able to identify real cyber-attack attempts and act according to procedures learned and already practiced in a simulated environment. On the other hand, cybersecurity experts need to be trained based on current situations, using advanced technologies and techniques (which an attacker would have at their disposal). Performing training and testing in a simulated environment, configured according to current requirements is a key factor in anticipating critical situations in terms of cybersecurity.

4. Cyber range as a cyber security training platform

Cyber range systems can be successfully implemented and configured to serve as a training platform for cyber security engineers but also to educate regular users to anticipate their involuntary participation in a successful cyber-attack. Figure 3 shows an overview of the use of cyber range systems as a training instrument for users and experts in cybersecurity, on the one hand, and the testing of IT infrastructures (from the perspective of cybersecurity) on the other (European Cyber Security Organisation (ECSO), 2020).

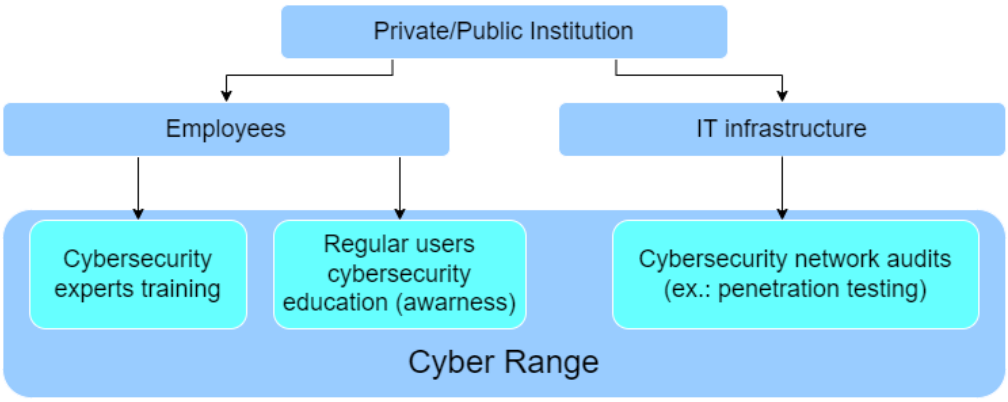

Figure no. 3. Cyber Range as a cybersecurity platform

When it comes to a company's/public institution's cyber security, there are two main players: IT infrastructure and employees (users - from the IT perspective). As previously presented, recent studies show that the lack of awareness of the risks regarding cyberattacks and computer systems misconfigurations are the main factors in computer data breaches. Cyber range systems implementations may serve both as a training instrument and network audit platform. Employees (as IT infrastructure users) training through practical methods can be easily done using a cyber range system. Within a cyber range, multiple and diversified scenarios can be developed. During the execution of these scenarios, the students can be part of some simulations of real-life situations that they might face during the activities performed at work. Moreover, the computer network in which the users carry out their activity can be replicated so that the scenarios played are as realistic as possible. In this way, users will participate in these training sessions without having to contact an unknown network, in which they would not feel comfortable or would not find themselves with the undertaken activities. From the perspective of training cybersecurity specialists, complex and current scenarios can be implemented within cyber range systems, configuring virtual networks that have diversified technologies and software applications. In this way, specialists will learn skills that will facilitate the prevention of cyberattacks and prompt and effective response in case of detection of such attacks. Last but not least, cyber range systems can be an important factor in preventing cyberattacks and data leaks by providing IT network replication mechanisms for cybersecurity auditing. Network auditing process may contain dangerous actions which can directly affect the production environment. The ability to make a virtual copy of the target network is an important advantage as complex infrastructure tests can be performed without considering the problems created by a possible down-time of the network. From stress tests to exploiting complex vulnerabilities (identified in the audited network), all actions are performed on the virtual replica of the network. Also, to simulate a complex scenario, network auditing can overlap with user involvement and their reaction testing in a cyberattack situation.

Recent studies reveal a classification of the cyber range systems, from the provided IT infrastructure perspective:

- *Simulation cyber range systems* - the implemented system offers virtual network infrastructures that are deployed according to the requirements of the present scenario or purpose; virtual environments are not replicas of actual IT infrastructure and do not provide a mirroring of production systems and services;

- *Emulation cyber range systems* - unlike simulation CRs, emulation provides virtual infrastructure copies of real networks, systems, and services; it can be used to deploy virtual copies for critical network infrastructures in order to perform security audits that would have a significant impact on performance if run on the production environment; it can also be used to implement and test hypothetical scenarios without putting the production network at risk;

- *Mixt cyber range systems* - this approach combines simulation and emulation to provide complete solutions tailored to an organization's needs; it can be used to deploy virtual infrastructures that are based on real networks but also enhanced with simulated new systems and services; it provides a proper infrastructure for testing simulated scenarios on virtual copies of sensitive real networks; it is the safest way to perform risky audit actions, to test the integration of new systems, and to test the integration of new systems.

To fulfilling the purpose for which it is implemented, a Cyber Range must provide a set of characteristics regarding (European Cyber Security Organisation (ECSO), 2020):

● *Realism and fidelity* - must be folded as much as possible for training purposes - in network testing, CR must allow 1:1 virtualization of the real network (physical or virtual); in simulation cases, CR must provide the complete set of tools and methods to deploy sophisticated virtual networks;

● *Accessibility and usability* - accessible in order to participate in a service or training offered on such a system; adaptable to a new group of users; depending on the level of information access, accessibility may vary from organization to organization - CR implementation must be tailored to the specific needs and regulations of the organization;

● *Scalability and elasticity* - the system must be able to grow both structurally and by building new components / features that can easily be integrated with the existing system, as well as the ability to swiftly embrace new technologies.

Self-paced learning courses are another area where cyber range systems may be employed successfully. This time, the configured scenarios will be dependent on the course curriculum that the user is enrolled in. In cybersecurity classes, situations may be identical to those mentioned above, or they may include practical exercises to reinforce theoretical concepts acquired concurrently. There are several cyber range systems that successfully service such corporate tasks. Offensive Security, EcCouncil, HackTheBox, and other well-known firms provide high-quality cyber range instruction.

5. Cyber range in Competency-based-Education

● on-the-job experience by simulating real life scenarios that can cover a wide range of environments, from simple to critical ones (Kellogg, 2018);

● real time performance feedback as the cyber ranges participants can be monitored by trainers or experts in this field while going through the exercises; also, participants get real time feedback on their progress and results

● training exercises intended to a wide range of participants, from non-technical staff to Cybersecurity professionals; there is great flexibility on designing scenarios that can fit any training goals and any participant profile;

● a dynamic training environment that can be easily changed and adapted to cover classic scenarios or new technologies

● a low-risk and a low-cost training environment that can simulate real infrastructures;

● a collaborative learning environment as participants can work in teams or individually against other teams or against actors managed by Artificial Intelligence.

From a CBE perspective, Cyber Ranges provide a dynamic and skills-oriented environment that can cover multiple learning approaches:

● problem-based learning as trainees need to solve independent problems which have clearly defined goals;

● project-based learning that cover complex scenarios that can require interdisciplinary knowledge and in which trainees go through a series of interconnected stages and interact with different systems and solutions

● experimental learning as the cyber range allows participants to test new technologies, new environments and new techniques for defense and attack;

● challenge-based learning environment where private or public companies can provide real-life scenarios, relevant for different industries and public infrastructures.

Some of the most important principles of the competency-based education (CBE) are reflected in the way a cyber range provides the learning environment:

● participants can learn at a variable pace as the resources are always available locally on students' computers, in the institutional private cloud or in public ones. Deadlines and limited time frames to access those resources can be imposed but for Cybersecurity training the quality and the volume of the acquired knowledge is more important than getting as much information as you can in a limited time;

● participants are supported in their learning getting real-time feedback from instructors that can monitor their activities or from software tools;

- effective and practical-skills oriented learning resources are available all the time
- exercises are reusable and new ones can be derived with minimum effort
- problems to be solved reflect real-world problems
- assessments are secure and reliable as they evaluate the practical ability of students to solve problems and not to reproduce knowledge.

Studies done by Kellogg (2018) and Strategy Labs (2021) have highlighted the main differences between traditional education and Competency-based-Education. Cyber Ranges as educational tools fit in the CBE environment as their role is to help students to get practical knowledge and skills. Table 1 describes the perspective provided by cyber ranges.

Table no. 1. Comparing Traditional Education and Competency-based-Education in Cybersecurity with cyber ranges

Traditional Education	Competency-based-Education in Cybersecurity with Cyber ranges
Course that delivers facts	Competency and practical skills/abilities
Based on in-person or online courses, laboratories. Has a limited time and it covers a predefined set of problems	Students can use every available source of information or open education resources as many exercises and problems may require interdisciplinary knowledge covered by different computer science courses. Can take place online or face-to-face in laboratories. Can be self-paced. It is a dynamic environment that can be flexible and tailored to adapt to different requirements
Assessment based on exams and projects. Focused on solving predefined sets of problems in a limited time.	Evaluation based on determining the level of competencies and skills gained at the end of the program. The evaluation environment provided by the cyber range can be dynamic, it can adapt and react to student actions. The assessment is outcome-based.
Mostly individual	Individual and collaborative (team-based) activities
Teacher centered	Student or team centered
Progress is measured by reaching course milestones in a fixed time. Students must demonstrate they know the presented facts	Progress is done by demonstrating that they can apply what they learned.
Based on passive and active learning	Based on active learning
Driven by accumulating as much information from textbooks and other provided resources	Driven by research as information needed to solve the given scenarios can't be provided by a single course. Many bits of information is provided by white papers, software documentation, technical blogs, forums and other outside the class resources.

Conclusions and future work

The accelerating progress in the cyber sphere necessitates ongoing training in cyber security, both at the user and expert levels. The more complicated the environment in which users operate, the more difficult it is to create a suitable training environment in which they are finally effectively educated to considerably enhance the degree of cyber security inside the organization. Hands-on activities carried out in a simulated/emulated environment, very comparable to trainee's day-to-day activity settings, are more effective than traditional training methods. Cyber Range systems, when used as a competency-based education instrument, may significantly improve training performance in the field of cybersecurity. Cyber Range systems may be developed in such a manner that the training scenarios are as realistic as possible, up-to-date, and impactful, regardless of the level at which the training is carried out: people who handle existing technology in the work environment or cybersecurity specialists prepared to handle latest threats/vulnerabilities that can harm their networks. To summarize, cyber range systems cover a wide range of cybersecurity scenarios and sub-domains, which is why they can be used to effectively support cybersecurity training programs. The current study is beneficial because it exposes elements that might

increase computer system users' awareness of the risks of cyber security incidents, on the one hand, and cybersecurity specialists' training, on the other. This research limitations consist of the lack of a practical study on a group of users and cybersecurity specialists who are trained using cyber range systems and monitored to see whether there is significant progress compared to a similar group who have gone through the conventional learning process. This work may be expanded by performing a study to determine the influence of cybersecurity training on cyber security incidents minimization. Following that, a study based on this data may be performed to determine the impact of adopting cyber range systems vs traditional training techniques. Also, research to compare the expenses of implementing a cyber range system for cyber security training to the resources (time and money) saved by staff training can reveal real advantages of such educational instruments.

Acknowledgement

This paper was co-financed by The Bucharest University of Economic Studies during the PhD program.

References

Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G. and Ferrag, M.A., 2021. Cyber Ranges and TestBeds for Education, Training, and Research. *Applied Sciences*, [online] 11(4), p.1809. https://doi.org/10.3390/app11041809.

Columbus, L., 2020. *What Are The Fastest Growing Cybersecurity Skills In 2021*?, [online] Available at: <https://www.forbes.com/sites/louiscolumbus/2020/11/01/what-are-the-fastest-growing-cybersecurity-skills-in-2021/> [Accessed 12 February 2022].

Dieck-Assad, G., Ávila-Ortega, A. and González Peña, O.I., 2021. Comparing Competency Assessment in Electronics Engineering Education with and without Industry Training Partner by Challenge-Based Learning Oriented to Sustainable Development Goals. *Sustainability*, [online] 13(19), p.10721. https://doi.org/10.3390/su131910721.

European Cyber Security Organisation (ECSO), 2020. *WG5 PAPER Understanding Cyber Ranges: From Hype to Reality*, [online] Available at: <https://www.cyberranges.com/whitepaper-download-understanding-cyber-ranges-from-hype-to-reality/> [Accessed 12 February 2022].

IBM, 2021. *Cost of a Data Breach Report 2021*, [online] Available at: <https://www.ibm.com/security/data-breach> [Accessed 08 February 2022].

Irwin, L., 2022. *Data breaches and cyber attacks in 2021: 5.1 billion breached records*, [online] Available at: <https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-in-2021-5-1-billion-breached-records> [Accessed 16 February 2022].

Kellogg, S.E., 2018. *Competency Based Education: Best Practices and Implementation Strategies for Institutions of Higher Education*, s.l.: Doctorate in Education. Concordia University St. Paul.

Klein-Collins, R., 2016. *Faculty and administrator views on competency- based education: A report from CAEL's jumpstart initiative*, s.l.: CAEL.

Malonda, C.K., 2022. Application of the Competency-Based-Education in the Electricity Option by Teachers of Optional Courses at Salama Technical Institute. *American Journal of Educational Research*, 10(1), pp.27-38.

Pham, C., Tang, D., Chinen, K. and Beuran, R., 2016. CyRIS: a cyber range instantiation system for facilitating security training. In: *Proceedings of the Seventh Symposium on Information and Communication Technology*. [online] SoICT '16: Seventh International Symposium on Information and Communication Technology. Ho Chi Minh City Vietnam: ACM.pp.251–258. https://doi.org/10.1145/3011077.3011087.

Purplesec, 2021. *2021 Cyber Security Statistics: The Ultimate List of Stats, Data & Trends*, [online] Available at: <https://purplesec.us/resources/cyber-security-statistics/> [Accessed 11 February 2022].

Strategy Labs, 2021. *Understanding Competency-based education. State Policy to Increase Higher Education Attainment*, s.l.: Education Commission of The States.

US Bureau of Labor Statistics, 2022. *Occupational Outlook Handbook*, [online] Information Security Analysts: US Bureau of Labor Statistics. Available at: <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm> [Accessed 11 February 2022].