https://doi.org/10.48009/3_iis_2019_186-193

Issues in Information Systems
Volume 20, Issue 3, pp. 186-193, 2019

INCREASING THE EFFECTIVENESS OF THE CYBERSECURITY TEACHING AND LEARNING BY APPLYING ACTIVITY THEORY AND NARRATIVE RESEARCH

Constanta-Nicoleta Bodea, The Bucharest University of Economic Studies, bodea@ase.ro
Maria-Iuliana Dascalu, University Politehnica of Bucharest, maria.dascalu@upb.ro
Mihail Cazacu, The Bucharest University of Economic Studies, mihail.cazacu@gmail.com

ABSTRACT

Several studies indicate that companies are still facing with severe challenges in recruiting specialists in cybersecurity, for protecting the companies' systems from cybersecurity attacks. These challenges are caused by the existing gap between knowledge, practical experience, and critical soft skills as developed by the cybersecurity educational programs and trainings and the real needs of the companies. The increase of the effectiveness of teaching and training in developing the students' skills as required by the companies becomes more and more important. The paper aims to present the challenges of applying the Activity Theory and the narrative research in improving the effectiveness of teaching and learning processes in a master degree program on Cybersecurity, delivered by the university where two of the co-authors are working.

Keywords: Cybersecurity education, Activity Theory, Narrative research, teaching and learning effectiveness.

INTRODUCTION

Information systems are increasingly being affected by security breaches, data disruption or unauthorized usage. The Report of Privacy Rights Clearinghouse (2018) mentions that in 2018, only in the United States over 8,000 data breaches were reported since 2005, with more than 10 billion records affected. According to IBM Security and Ponemon Institute (IBM, 2018), the average cost of a data breach exceed 3.86 million US dollars, with 6.4% as the average cost increase per year. As a reaction to these treats, the organizations set up specialized units for dealing with the security issues, so called Information Security Operations Centers (ISOCs). ISOCs have specialized personnel supervising information systems in place, by using specialized monitoring and controlling tools.

Considering the technological advanced tools and the continuous changes in the security breaches, a high level of personnel qualification and a continuous professional development are required. The effectiveness of education programs and trainings in cybersecurity in developing the students' skills is an important requirement of the companies hiring the cybersecurity specialists. Different solutions were proposed for increasing the effectiveness of teaching and training in cybersecurity. Recent studies (Sundaramurthy et.al, 2016; Sundaramurthy et. al, 2014) shown that the Activity Theory can contribute to the improvement of teaching and learning, by guiding the identification and the resolution of inherent tensions/conflicts arising in the educational activities. Activity Theory is only the conceptual framework for addressing the quality issues. In order to apply it for specific educational or training settings, additional specific research methods for collecting and analyzing data should be applied.

The paper aims to present the challenges of applying the Activity Theory and the narrative research in improving the effectiveness of teaching and learning processes in a master degree program on Cybersecurity, delivered by the university where two of the co-authors are working. Since 2005, the Bucharest University Studies offers a master degree program in Cybersecurity, the initial name being IT&C Security (http://ism.ase.ro/). The program is delivered in English. More 1100 professionals graduated of this program. The mission of the program is to share theoretical knowledge and to insure the practical technological transfer from Cybersecurity domain among the developers, administrators, project managers and users of the electronic devices eco-system. Also, the program intends to rise the security and reliability level of development and deployment of e-Systems taking into consideration the risks of cyber-attacks and specific issues.

The paper is structured as follow: Section 2 presents the current challenges that cybersecurity education and training are facing in our days. The next section presents the relevance of the activity theory in the context of increasing quality of teaching and learning. Section 4 present the research methodology, followed by the presentation of the results. The Conclusions presents the directions of the future research.

CURRENT CHALLENGES IN CYBERSECURITY EDUCATION AND TRAINING

The CSIS survey, conducted in 2016 revealed that only 23% educational programs which are available in US are fully preparing the graduates for a cybersecurity career (Evans and Reeder, 2016). In 2018, the ISACA association found that 61% of organizations participating in a survey declared that less than half of the applicants for cybersecurity jobs were qualified for the job (ISACA, 2018). In 2019, the CSIS report indicates that companies are still facing with severe challenges in recruiting specialists in cybersecurity, for protecting the companies' systems from cybersecurity attacks (Crumpler and Lewis, 2019). These challenges are caused by the existing gap between knowledge, practical experience, and critical soft skills as developed by the cybersecurity educational programs and trainings and the real needs of the companies.

But what are the real needs of the companies concerning the profile of the cybersecurity specialists? Dawson and Thomson (2018) reviewed different studies on competence profile of the cybersecurity professionals and they concluded that only a proper mix between technical knowledge and soft skills can insure a successful performance, at individual and team levels. The cybersecurity professionals must have extensive technical knowledge in computer operating systems and networks, ready to be applied in a specific local environment (so called situated knowledge). Also, they have to have strong abilities in the usage of analytical tools for the networks scanning and mapping and for vulnerability analysis. They also must have pattern matching abilities and flexibility, which are required for scanning a large number of network events/alerts, which appear on different computer screens. Strong analytical skills are needed for dealing with information coming from different sources and for judging the network activity and the network health status and for assessing the cybersecurity risks. And, of course, they need to have soft skills, allowing them to efficiently work in teams, to be able to communicate, to solve conflicts, to be predictable and reliable.

In order to close the existing competence gap in the cybersecurity domain, several frameworks for designing the cybersecurity programs or trainings were proposed, based on the analysis of the current practices. One current practice for trainings that is expanding in our days, including in cybersecurity training is apprenticeship. Apprenticeship is expanding training in the entire IT industry, not only in the cybersecurity training (Zakrzewski, 2019). A consortium consisting of seventeen companies, including IBM, Canon, Ford and Bosch decided to use apprenticeships for addressing the training/retraining needs of thousands of their workers. IBM already launched an apprenticeship program in 2018. It is a new approach for IT, considering that the apprenticeship was not very much applied in IT in the past, but mainly in manufacturing. In several countries, these apprenticeship programs are financed by the government, for example, IBM ran different apprenticeship programs registered with the US Labor Department. The programs has usually one year duration. The main advantages of these programs are that they develop specific job skills and a strong connection of the participants with the organization work values. At the end, they deliver well-trained and reliable employees. The apprenticeships are suitable not only for young high school or college graduates, but also for experienced professionals with different background, looking for new jobs. By attracting such diverse workers, IT companies can take benefits from this diversity, by improving the creativity potential. The main characteristic of apprenticeship programs is that learning is achieved by practicing on real-world tasks.

In (Beuran et. al, 2016), some Japanese experiences in cybersecurity training are presented. The authors analyzed several training programs, including enPiT-Security (SecCap), CYDER, and the Hardening Project. These programs are described from the point of view of the applied training practices and methodologies. Three main categories of trainings were identified: attack-oriented training (including practical exercises on the penetration testing, using the tools and methodologies used by attackers), defense-oriented training (focusing on the vulnerability protection mechanisms, in order to prevent the future attacks) and analysis/forensics-oriented training (aims to develop a deeper understanding of the vulnerability exploitation and patching). All training activities are based on the real-world incidents. For simulating incidents, complex network environments are usually needed, for emulating the real

context in which these incidents occur, especially the computers' settings and the network topologies. The simulation of real incidents during the training is considered as being the main factor in increasing the effectiveness of trainings.

Other approaches which are applied in the cybersecurity teaching and learning are gamification and Virtual and Augmented Reality (Gonzalez, Llamas and Ordaz, 2017). Computer security competitions, such as Capture the Flag (CTF) contests represent an efficient way for introducing and exercising some of the cybersecurity topics. Several open source frameworks for deploying Capture the Flag contests are already available. Other similar cybersecurity training resources are: Hacking-Lab, Smash the Stack Wargaming Network, W3Challs, Hack.me, HackThis and RuCTF

One of the most important issue in the current cybersecurity training practices is the high training related costs. The main cost categories of trainings in cybersecurity are the following: equipment costs, setup costs and content update costs. The setup costs for equipment and environments tend to become higher that the equipment costs, due to the fact that the configuration tasks are knowledge intensive and most of the time manually performed. In addition, the cyberattacks' characteristics are changing in a short period of time, leading to the requirement to frequently update of training content, which also rise the training costs. In order to reduce costs, many trainings are done on desktops and obsolete incidents, which lead to a reduced effectiveness of these trainings. A solution for reducing this high resource demand in cybersecurity trainings is to apply e-learning tools, developed by using machine learning techniques. By using these tools, the setup and content update costs can be reduced and a training effectiveness can be improved.

The effectiveness of an education and training program can be defined as adequacy of the content and applied teaching and learning methods to the level of knowledge, skills and abilities intended to be reached by the participants at the end of the program, under the condition of an appropriate report cost/performance, so that the program to be sustainable on long term (Beuran et. al, 2016).

Evaluating the effectiveness of the process of teaching and learning implies studying the complex interactions involving teachers, students and the employers those students would work for after graduation. Activity Theory does offer the framework to study teaching and learning of any IT topics in general since in IT the human activities are always mediated by tools (hardware, software and what Activity Theory calls "psychological tools", which are theories, algorithms, heuristics, etc). Moreover, both the teaching-learning process and the subsequent work of the graduates of the IT classes happen according to sets of rules, happen in communities (class, company) and imply division of labor (e.g. teachers, students, managers, subject matter experts, tier 1, tier 2 analysts, etc).

APPLYING ACTIVITY THEORY FOR EVALUATING THE EFFECTIVENESS OF CYBERSECURITY EDUCATION AND TRAINING

Activity theory proposes a standard view for activities. Each activity is described with the following components: outcome, object, subject, instrument, rules, communities and division of labor. For education and training activities these components have a specific instantiation, as it is shown in figure 1.

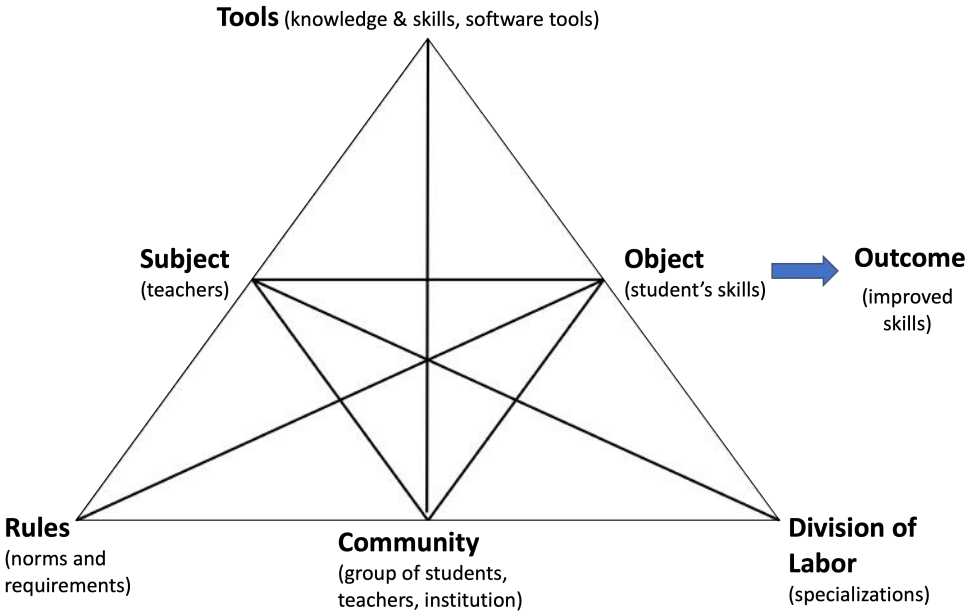

Figure 1. Activity theory applied in teaching and learning

The Activity Theory is applied in educational research mainly due to its modelling power. The complex teaching and learning interactions are represented using standard components (Tools, Subject, Object, Rules, Community and Division of Labor) and relationships between all these components (Thorgeirsdottir, 2015; Cazacu et al, 2019; Li and Cargill, 2019). These relationships are characterized by contradictions (tensions), such as between subject and tools (for example, when the teachers are facing difficulties in using educational tools), subject and community (for example, when the teacher has to work with a big size class). It is common to consider these tensions as being systemic, in a sense that they are affecting the effectiveness of the entire process of teaching and learning. These tensions between each pair of elements included in the model can have specific causes and occurrences in different educational and training situations. The way how a tension occurs is influenced by a "mediating" component, which creates the context and/or represents the trigger for that specific contradiction/tension. Figure 2 shows the systemic tensions between the different model components of teaching and learning. The figure shows not only the two components being in contradiction, but also the mediating element.

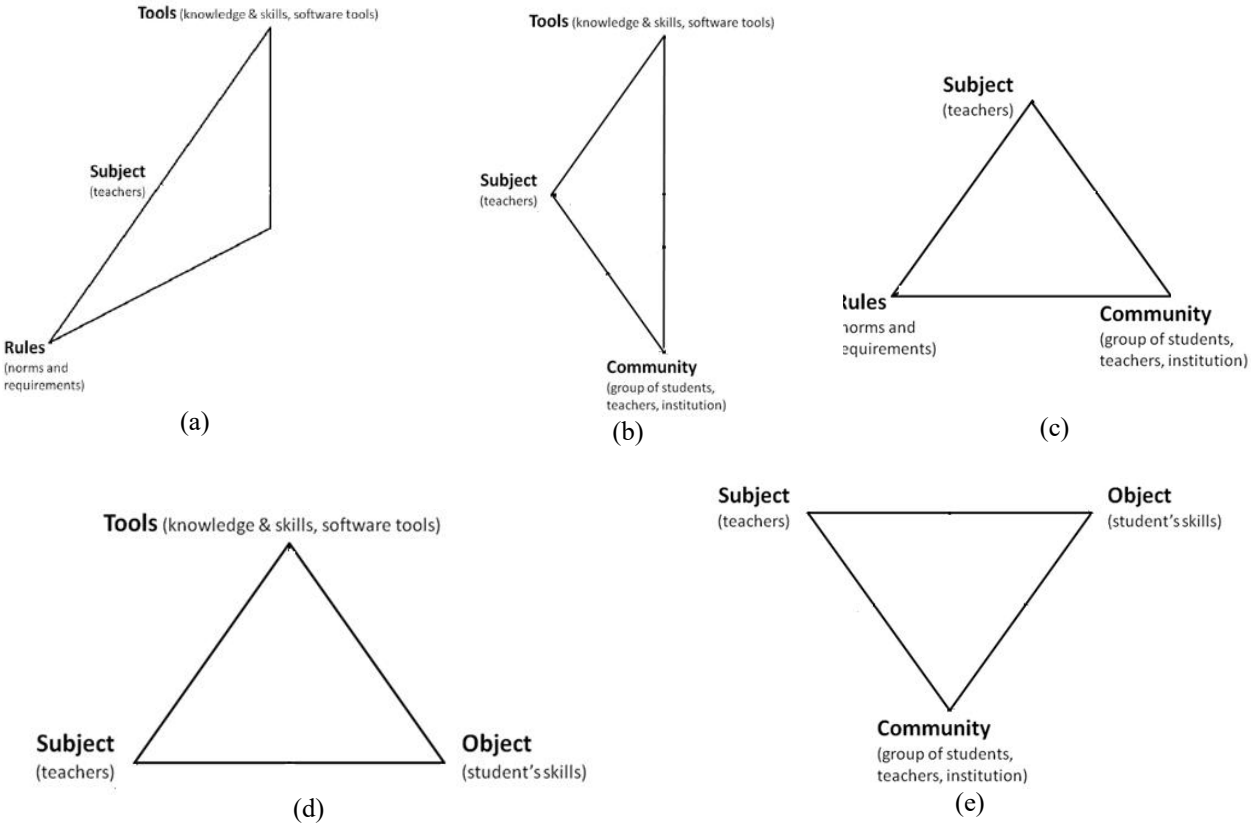

Figure 2. Examples of systemic tensions/contradictions in teaching and learning activities

According to the Activity Theory the tensions/contradictions represent the source of the education and training practices progress. The underlying assumption is that by solving these tensions, the effectiveness of teaching and learning is gradually increased. But in order to solve the tensions/contradictions in specific education program or training and in order to test the assumption that solving those contradictions does increase the effectiveness of teaching and learning, data about the teaching and learning practices, as they are performed should be collected and analyzed.

RESEARCH METHODOLOGY

The research was guided by the following question: How the skills of the students in cybersecurity can be better improved through a more effective teaching and training in the master degree program? Using the Activity Theory framework, we have decided to focus on teachers as the Subjects of the Activity Theory Model, to identify the actual materialization of the contradictions represented in Figure 2 and see if we can identify the measures to be taken in order to bring about progress. This are leading to several findings which in the subjects' opinion impacted the effectiveness of the process.

In order to decide on the data collecting and analyzing approach, we took into consideration the following methods: the narrative studies, the ethnographic studies and the case studies. In Activity Theory Parlance, those are the Tools the Subject (the researcher) uses to operate on the Object (the complex system of teaching and learning cyber security) in order to obtain the Outcome (ways of increasing the effectiveness of the learning process). In a narrative study, the respondents are encouraged to reflect about their experiences as teachers/students in their own pace and time, returning to the testimony offered when they want to change it. Thus reflection takes place over a longer period of time than it happens usually in an interview. The ethnographic studies represents a research about different patterns and perspectives in the environment where they can be observed. For teaching and learning, the

ethnographic studies can be organized as class observations and reflections. The case studies represent in-depth investigations of specific processes/phenomena, in order to better understand these processes/phenomena and to develop the theory.

After taking into account the actual constrains on time and resources we opted for the narrative study. The participants in the narrative research were three of the teachers involved in the master program: one teacher having less than 5 years teaching experience in the university, but an extensive experience in IT companies, in the field of cybersecurity, one teacher having 15 years experience in teaching in university and collaborating with IT companies for different projects and the other teacher having more than 30 years experience in teaching, extensive theoretical knowledge but limited collaboration with IT companies.

The following topics were designed to guide the reflection of the participants:

- Which is the role of theoretical knowledge and practical experience in teaching the cybersecurity disciplines (challenges which the teacher with limited theoretical knowledge or limited practical experience has to face with during teaching)?
- What is the influence of confidence in using different software tools (for simulating incidents, emulating the real context in which these incidents occur, penetration testing etc.) on the teaching effectiveness?
- What is the impact of organizational rules on the usage of different software tools?
- How important is the support offered by university?
- What is the impact of the big class size on the tools usage?

The participants were invited to reflect on these topics for two weeks. They were advised to consider that the value of the data comes from personal experience and examples. They were also invited to include any issues that might concern them and which were not included in the guide, issues which required their effort or which have been solved (because personal experience is the one that matters).

After two weeks the stories of the teachers were received and the interpretation phase started. In order to interpret the narratives, the following analytical approaches might be applied: thematic analysis, structural analysis, dialogic/performance analysis and visual narrative analysis. In this case, the first approach, the thematic analysis was applied. The main findings are presented in the next section.

MAIN FINDINGS

The narratives analysis reveal the following teachers' perceptions of challenges and solutions to these challenges:

Role of theoretical knowledge and practical experience in teaching the cybersecurity disciplines
All teachers considered lacking knowledge and practical experience a major challenge in teaching. The more experienced teacher valued more the theoretical knowledge, but he admitted that practical experience is absolutely necessary in teaching cybersecurity. The younger teachers valued more the practical experience.

> "*As professionals we have the ability to learn from a handful of examples. This means that once we find out the correct way to deal with a new threat, this knowledge could be passed to others before there are enough incidents accumulated to generate a new Tool. Knowledge transfer happens if the knowledge-holder has the ability, time and willingness to pass it. This is what is happening in training sessions.*"

In figure 2(d), the challenge of lacking theoretical knowledge and/or practical expertise is represented as a tension Tools and Subject, mediated by Object (the skills which are intending to develop by using the knowledge and practical expertise)

Influence of the confidence in using different software tools on the teaching effectiveness
Using software tools was listed as a challenge in all narratives. The tools are mainly used for simulating incidents, to emulate complex network environments, for emulating the real context in which these incidents occur, especially the computers' settings and network topologies. The simulation of real incidents during the training is considered as being the main factor in increasing the effectiveness of trainings by all three teachers. In order to avoid lacking of

confidence, the teachers recommend the participation in projects. The collaboration with different IT companies offers opportunities for more experience in the tool usage and access to high technology tools, before these tools to be adopted as educational tools by the universities.

In figure 2(d), the challenge of lacking confidence in using different software tools is represented as a tension Tools and Subject, mediated by Object (the skills which are intending to develop by using the knowledge and practical expertise)

Impact of organizational rules on the usage of different software tools

> *"The organizational rules are quite similar for all disciplines, regardless of the disciplines' particularities. I will rather prefer to work in a modular manner, which means to stay in the IT laboratory with my students for 6-8 hours instead of meeting them once per week for only two hours. But the organizational rules do not allow us to choose the former. In two hours, the students can't run to many simulations and it is hard to get results and to interpret them. Therefore, even if there are tools available, their usage is limited due to administrative reasons."*

> *"I would like to go with my students in one of the company that I collaborate with, for a practice stage. But the administrative regulations make this very difficult to be organized. So, we are staying in the university for all classes, even if the companies have a more dynamic, with more tools and examples, providing students with a more interesting environment for teaching and learning.*

In our interpretation, these comments imply lacking of flexibility of organization rules. In figure 2(a), the challenge of having in place rigid organizational rules is represented as a tension between Tools and Rules, mediated by Subject.

Importance of the support offered by university, at different levels
Narratives indicate some support offered by the university, faculty and department running the program. Nevertheless, different administrative challenges led to a lack of support for teacher of the cybersecurity program at different hierarchical levels. The perception of teachers is that this lack of support is explain by the lack of understanding about the specificity of the program in comparison with other programs offered by the university.

The challenge of lacking support from university, at different levels is represented in figure 2(c) as a tension between Rules and Community, mediated by Subject and in figure 2(e) as a tension between Community and Object, mediated also by the subject

Impact of the big class size on the tools usage
The teachers identified several issues surrounding students.

> *"In each of my classes there are more than 30 students enrolled. It is difficult to organize properly the activities in such big class size, especially to monitor the students' performance, also, it is difficult to answer their questions when they face unknown-until-then situations"*

In figure 2(b), the challenge is represented as a tension between Tools and Community, mediated by Subject.

CONCLUSIONS

Activity Theory is used as both a descriptive and investigative approach for investigating complex human activities, like teaching and learning. As a descriptive tool it allows the activity to be represented as a collection of components with relationships, described by a directed path through the nodes (activity components) of the graph. As an investigative tool, the Activity Theory indicates where the problems and their solutions may be found. According to the Activity theory, each edge of the graph can indicate a potential "tension/contradiction" that can be better understood considering a mediating factor. The application of Activity theory in a specific educational environment requires methods for collecting and analyzing data about teaching and learning processes. The narrative is a qualitative research method allowing a deep understanding of the educational processes.

The narrative research conducted by the authors in a master degree program in cybersecurity reveals some of the challenges faced by the teachers. Despite of the teacher profile differences, related to the level of seniority in teaching and the practical expertise, their perceptions are very similar in regards with the investigated topics.

Even if teachers acknowledged the challenges, they didn't consider that these challenges are easy to be solved, mainly due to the lack of understanding of the particularities in delivering education in this specialization at the university level. The teachers proposed that foreign teachers to be invited by the university to deliver presentations about the cybersecurity education and training state of the art. This would increase the level of understanding at different university levels about the requirements for an effective cybersecurity program.

The actual research covers only a few potential contradiction/tensions. In the future, the authors intend to extend their research to other components of the educational activity model. Also, the other stakeholders (new Subjects in the Activity Theory framework), such as students and employers will be invited to offer data. New Tools like ethnographic studies could be envisaged for studying the interactions in class and at work. By extending the scope of the research, the authors should reconsider the research methodology to be applied, because the narrative research is not fitting very well for a large number of topics and for other categories of stakeholders, such as the university leaders or managers of ISOCs.

REFERENCES

Beuran, R., Chinen, K., Tan Y., Shinoda, Y. (2016). *Towards Effective Cybersecurity Education and Training*, Research report, IS-RR-2016-003, Japan Advanced Institute of Science and Technology (JAIST), Ishikawa, Japan, October.

Cazacu, M., Bodea, C.-N., Dascalu, M.-I., Cucu, C. (2019). Using the Activity Theory to Identify the Challenges of Designing Elearning Tools based on Machine Learning for Security Operations Centers, in: *Proceedings of The International Scientific Conference eLearning and Software for Education Conference,* Bucharest**,** 1, 452-461.

Crumpler, W., Lewis, J. A. (2019). *The Cybersecurity Workforce Gap*, Report of Center for Strategic and International Studies, January, https://www.csis.org/analysis/cybersecurity-workforce-gap

Dawson, J., Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance, *Frontiers in Psychology, 9*, Article 744, June.

Evans, K., Reeder, F. (2016). A Human Capital Crisis in Cybersecurity*,* Report of Center for Strategic and International Studies.

Gonzalez, H. Llamas, R., Ordaz, F. (2017). Cybersecurity Teaching through Gamification: Aligning Training Resources to our Syllabus, *Research in Computing Science, 146*, 35–43.

IBM Security and Ponemon Institute (2018). https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf

ISACA (2018). *State of Cybersecurity, Part 1: Workforce Development*, Report of Information Systems Audit and Control Association, April.

Li, Y., Cargill, M. (2019). Observing and reflecting in an ERPP "Master Class". Learning and Thinking about application, in: Corcoran, J.N., Englander, K. and Muresan, L.-M. (2019), *Pegagogies and Policies for Publishing Research in English*, ESL & Applied Linguistics Professional Series, Routledge, Taylor & Francis, NY.

PRC (2018). Data Breach Notification in the United States and Territories, https://www.privacyrights.org/blog/data-breach-notification-united-states-and-territories

Sundaramurthy, S.C. McHugh, J., Our, X., Wesch, M., Bardas, A. G., Raj Rajagopalan S. (2016). Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations, *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), Denver*, 237-251

Sundaramurthy, S.C., McHugh J., Ou, X., Raj Rajagopalan, S., Wesch M. (2014). An Anthropological Approach to Studying CSIRTs**, i**n: *IEEE Security & Privacy*, vol. 12, issue 5, 52-60

Thorgeirsdottir, H. (2015). *Investigating the use of Action Research and Activity Theory to Promote the Professional Development of Teachers in Iceland*, PhD Thesis, University of Iceland.

Zakrzewski, C. (2019). *The Technology 202: Technology companies turn to apprenticeships in tight labor market*, The Washington Post.