MCIC '21

The 12th International Multi-Conference on Complexity, Informatics and Cybernetics

March 9 - 12, 2021 – Virtual Conference

PROCEEDINGS

Volume I

Edited by:

Nagib Callaos
Jeremy Horne
Suzanne Lunsford
Belkis Sánchez
Michael Savoie

IIIS

Organized by

International Institute of Informatics and Systemics

Member of the International Federation for Systems Research (IFSR)

TABLE OF CONTENTS
Volume I

Development of Game-Based Learning Scenarios for Social Engineering and Security Risk Management for SMEs in the Manufacturing Industry

Margit SCHOLL
Technical University of Applied Science Wildau (TH Wildau), Faculty of Computing, Business, Law
Wildau, 15745, Germany

Stefanie GUBE
Technical University of Applied Science Wildau (TH Wildau), Faculty of Computing, Business, Law
Wildau 15745, Germany

Peter KOPPATZ
Technical University of Applied Science Wildau (TH Wildau), Faculty of Computing, Business, Law
Wildau, 15745, Germany

ABSTRACT

With increasing digitization, information security (IS) is becoming an important issue for all employees working in companies and organizations. If the human factor is to be seen as strength rather than a weakness, appropriate awareness-raising measures are required. One way to raise awareness is through game-based learning (GBL), which can be used as an ongoing means of motivating employees to engage emotionally with the subject of IS and changing their online behavior accordingly. As part of the project *Mittelstand 4.0—Kompetenzzentrum Stuttgart* (Mittelstand 4.0—Competence Center Stuttgart), two analog GBL scenarios on the topics Social Engineering and Security Risk Management for SMEs are currently being developed over the period of a year, from April 2020 until March 2021. In this paper, the development process—including the phases prototyping, testing, and adaptation—are described and the prototype results shown. Testing analog prototypes in times of COVID-19 is particularly challenging. The experience gained in this mini project will be incorporated into the new three-year project *Awareness Lab SMEs (ALARM) Information Security*, which is funded by the Federal Ministry of Economics and has been running since October 1, 2020.

Keywords: Game-Based Learning Scenarios, Social Engineering, Security Risk Management, SMEs, Manufacturing Industry, COVID-19 Challenges

1. INTRODUCTION

There is no doubt that information security (IS) is key to all organizations. With the increase in digitization, IS is becoming an ever-more important issue for all employees, as is the competence of those responsible for it. However, the existing legal and regulatory requirements relating to security awareness are often only binding for large companies or, as in the case of the IT security law, depend on the particular sector of industry [1]. In a study from 2017, two-thirds of the small and medium-sized enterprises (SMEs) surveyed regarded IT security as highly important, while only 20 percent had already carried out IT security analyses [2]. For small businesses, in particular, management systems such as ISO 27000 or the BSI standard exceed their resources [3]. In the manufacturing sector, 36.8 percent of SMEs regularly conduct awareness training for their employees [2].

In many organizations, information security awareness (ISA) and the training of relevant competences (ISAT) are often limited to knowledge-transfer measures. However, measures to raise awareness and conduct training on the abstract issues of IS do not seem to have a lasting effect: users do not always behave in the way they are supposed to [4]. Tsohou et al. (2012) [5] conclude from recent global security surveys that ISAT are not working at present. In many cases, a "technocratic" view of risk communication blocks the way to actual communication—in other words, there is a tendency for technical experts to tell people what they ought to know [6].

Moreover, policies that end up as long lists of dos and don'ts do not inspire employees. "Most employees only access [the policies] when they have to complete their mandatory annual 'security training' […], which has little to no effect on their security behavior" [7]. In addition, a one-time training aimed at addressing security awareness gaps is not sufficient to ensure the necessary compliance with the security culture [8]. However, psychological research shows that in addition to the classical theoretical approach to knowledge transfer, we need a marketing-oriented approach to promote emotional identification and a systemic approach to team-based communication [9] [10]. Because IS and IT are about more than technology [11] [12], social participation in a communicative team process seems to be a key component in developing ISATs and relevant training material.

This is where Serious Games and the game-based learning (GBL) methodology come in. GBL has great potential to make valuable contributions to socially relevant areas such as education and health [13] [14]. For this reason, it has been receiving increasing recognition over the last decade as an effective teaching and learning method that improves motivation and triggers behavioral changes [15]. Creating emotional resonance involves addressing specific individual concerns. People need to "understand"—through emotional engagement—that they are themselves affected by a lack of IS. Analog GBL is especially effective as a means of stimulating motivation and should be explicitly used for ISAT, because learners can directly see the consequences of their actions and get a sense of their knowledge level in dialogue.

Two analog game-based learning scenarios on the topics of social engineering and security risk management are being developed for SMEs in the manufacturing industry within the project *Mittelstand 4.0—Kompetenzzentrum Stuttgart* (Mittelstand 4.0—Competence Center Stuttgart). Our paper addresses central questions in the development of such analog learning scenarios for companies and how COVID-19 influences them.

2. METHODOLOGY

Game-Based Learning

The assessment of a risk according to its probability of occurrence and the potential extent of the damage it can cause plays an important role here. The methods used for the development of the awareness-raising measures are mainly GBL and accelerated learning. Like IS, games are rule-based and thus inherently capable of being adapted to suit a wide range of IS topics. In developing and devising these games, it is important to orient them to specific target groups [16] and adapt them to the appropriate lived environment. The individual GBL scenario should impart knowledge to the target groups, while also engaging them at an emotional level and enabling them to practice new behavior patterns in a protected environment. The inclusion of interactivity in the development of the scenario and the enabling of a verbal exchange between the participants about their expectations and experiences are of particular importance.

In this process, the complex reality must be presented in a greatly simplified manner so that the learning scenarios can be easily understood and played. At the same time, the key dangers must be recognized, and motivation for behavioral changes supplied. In order to further reduce complexity, familiar game mechanics or codes from pop culture are used in some cases to enable a quick grasp of the rules. The use of a moderator makes it possible for the topic to be quickly introduced. In addition, the moderator's presence guarantees the flow of the game and encourages discussion.

The goal of the developed learning scenarios is not to offer extensive training but to raise awareness among participants. While these measures provide a sense of IS and enable individual participants to recognize the importance of the topic, reflect on their own behavior, and respond accordingly [17], training courses aim to build deeper knowledge and skills.

First Phase: Creating Ideas

Various creative methods can be used as an introduction to the individual topics. One of the classic methods is brainstorming, in which ideas are generated without any criticism. A subsequent process of mind mapping helps to organize the ideas that have been generated and develop them further. The combination of individual and joint brainstorming in the group achieves particularly good results [18].

Although creative workshops had been included in the planning for the mini project as a means to set priorities for the learning scenarios, owing to the COVID-19 regulations, these could not take place. Instead, two surveys with SME-related organizations (a transfer agency and a nationwide working group on IS) served as a basis for developing the scenarios. The first survey served to specify the task, while the second contained questions on content. For 60 percent of the fifteen survey participants, analog GBL scenarios packaged as serious games have not been used in training or education to date. In the few cases where analog learning scenarios have been used, the experience was very positive. Specific questions were asked to help gain an overview of prior awareness-raising and training concepts. It turned out that the choice of methods corresponds to the common practice of passive knowledge transfer. Lectures, print media (e.g., posters and brochures), and webinars were mentioned as focal points.

For the 36 percent of SMEs where learning success is measured, evaluation and feedback questionnaires are the method of choice. The learning scenarios on the subject of social engineering are intended to enable the participants to recognize attacks and protect or defend themselves against them. The complex learning scenario on security risk management is intended to motivate employees to consciously accept risks instead of ignoring them.

While various scientific papers [19] [20] [21] and Kevin Mitnick's *The Art of Deception: Controlling the Human Element of Security* [22] were used as inspiration for the topic of social engineering, the BSI standard 200-3 [23] served as the basis for developing the game on risk management.

Second Phase: Prototyping

In contrast to digital games, analog games also include haptics. Communication is direct and does not take place via chats. This favors discussion between the participants—for example, to help clarify terms, negotiate a strategy, or analyze an error. The development of analog

as well as digital and hybrid GBL scenarios is an iterative process that goes through the steps of development, testing, and adaptation several times before the final version is available. While in the mini project the two learning scenarios are only developed in analog form, in the large three-year project, *ALARM Information Security*, a broad spectrum of analog and digital learning scenarios have been set up, and their effectiveness will be checked.

Learning Scenario 1—Social Engineering: In a recent study conducted by the German Federal Office for Information Security (BSI), 37 percent of the more than 1,000 companies surveyed stated that they had been affected by analog and digital social engineering, with the number of undetected cases estimated at almost half [24]. Thus, in terms of espionage, sabotage, and data theft, social engineering is one of the most common crimes committed. This clearly indicates a need to raise awareness among employees.

In the process of developing the learning scenario, the topic of social engineering (SE) needs to be considered from multiple perspectives. At the same time, it is important to avoid monotonous repetitive loops. Therefore, the method of circuit training used in previous projects was adopted, and the learning scenario was designed in three parts. A metaphor was sought to connect these parts: the use of terms from the world of theater stems from the original idea of developing a role play.

The game begins with a round of introductions within the framework of the prologue, which is designed in the form of cogwheel gears: a reference to the manufacturing industry. The first act of the Social Engineering Theater (SET) "Sketch" is designed as a role play, which is then supplemented by a card assigned to the player. The second act "Directing" is a digital video quiz designed as a warm-up. The third act "Backstage" uses planning techniques in the form of a modified sequence diagram.

Besides the content and the methods and game mechanics applied, the amount of time needed or estimated for the game is a key consideration. Our "5/5/5 method" was often used for the circuit training sequence in previous projects (5 minutes for the introduction, 5 minutes for playing, and 5 minutes for evaluation and discussion). However, this method is only suitable for short-term awareness-raising measures. Because the SE tackled in this project requires a higher degree of complexity, considerably more time must be planned. The total time for SET is 90 minutes. The prologue of about 15 minutes precedes the three acts of 20 to 30 minutes each. However, depending on the number, mentality, and previous knowledge of the participants, the time can be shortened. This flexibility is important when using serious games in companies.

Learning Scenario 2—Security Risk Management: Since there are many other risks related to IS, the introduction of a security risk management system (SRM) is highly recommended. Fenz et al. identified the following as some of the common problems encountered in implementing an SRM: asset inventory and countermeasures, asset value assignment, risk assessment, and the trade-off between risk and cost [25].

Since SRM is an extremely complex topic, an analog learning scenario cannot cover all the areas. The focus was thus placed on risk assessment. In the project, support work has been contracted out to the firm known_sense. Their practical experience indicates that in a typical company, managers are initially not as open to GBL scenarios as other employees. In order to make the introduction to the topic and the learning scenario more accessible for the middle-management target group, various elements of the well-known game of roulette were used to arouse the interest of managers.

Third Phase: Testing

Owing to the COVID-19 regulations, the workshops planned for testing the learning scenarios in analog form have not taken place as yet. Since feedback is indispensable for further development, the prototypes and their descriptions were sent to the client for individual testing. In addition, on-site tests were carried out with small groups of trainees from the central IT service provider for the State of Brandenburg (ZIT-BB) and first-semester students from the administrative informatics course (VIBB-20) at TH Wildau. These analog tests were done in compliance with the distance rules and the obligation to wear a mouth-nose cover.

For the follow-up project *ALARM Information Security*, short questionnaires were developed and filled out by the trainees and students in the course of a test. The survey is a first step in developing methods to measure the effectiveness of awareness raising and is to be repeated after six months in the larger project to allow conclusions to be drawn about the increase of awareness over time. The results will also provide the data basis for a matching method that uses partial order to map learning paths.

Online Workshops: On-site workshops were planned to test the learning scenarios in detail: for example, with regard to the game mechanics. These are not feasible in the foreseeable future either, owing to the current COVID-19 regulations. As an alternative, hybrid (analog and digital) workshops are planned online for January 2021. Hybrid, in this case, means that the participants all log in via a video-conferencing system, but the workshop moderators are on-site with the respective learning scenario that has been set up. The participants get involved by supporting the moderator in his role as an "analog avatar" in conducting the learning scenarios, even steering his or her decisions and discussing them with each other. The goal is not a simple live broadcast and is thus not based on the mere consumption of content as in a webinar but on the interactive and emotional involvement of the participants. To this end, online conference tools

such as Zoom, jitsi, BigBlueButton (embedded on our university's Moodle platform), and CiscoWebex were first tested in detail with regard to their functionality. Later on, these were also examined from the point of view of data protection [26]. The selection process ultimately restricted the online conference systems in question to BigBlue-Button and CiscoWebex, both of which are already running on our university's servers. For the first time, a high-resolution web camera as well as a camera tripod with a swivel arm and counterweight are to be used, which will allow for classical communication and a view of the playing fields at the same time.

To summarize Kerres (2020), it should be noted that analog formats cannot be converted 1:1 into digital formats and that digital formats should be designed in such a way that they take into account various restrictions—for example, with regard to the channels of perception [27]. Therefore, such a conversion was out of the question. Similarly, an exclusively digital version was not considered, as this would lose the analog character and would, in practical terms, turn the serious game into an entirely new game. To ensure active participation in the workshop, the total number of participants is limited to ten.

Learning Scenario 1—Social Engineering Theater: The online workshop on Social Engineering Theater is designed in three parts. In the first part, the "Prologue," the participants introduce themselves, while one of the moderators notes down the information on the cogwheels and then places it on the camera image. In the second part, "Sketch," one or two sketches are presented by two moderators instead of the participants. The group is then divided into two or three breakout rooms in the video-conference system, each with one moderator. In these rooms, the sketches are discussed and debated. The results are then presented. The third part of the first learning scenario, "Backstage," follows a similar principle: the moderators serve as analog avatars for the participants and carry out their instructions—e.g., labeling cards and placing them in specific positions.

Fig. 1 Online Workshop: Risk Roulette—explanation in the presentation (in German)

Learning Scenario 2—Security Risk Roulette: Owing to the higher degree of complexity, the online workshop on Risk Roulette is designed as a presentation of the learning scenario in stills (see figure 1). The presentation introduces different possibilities for game mechanics. The individual options are then discussed in breakout rooms and subsequently presented to all participants.

3. PROTOTYPING RESULTS

Social Engineering Theater (SET)
In this learning scenario, a three-person team of participants receives a prepared sketch focused on one of three different social engineering attacks. Each team member takes a role in the sketch as speaker, employee, or social engineer. The scene is presented in front of the entire group and subsequently discussed and debated with regard to the attack vectors used, the social engineering techniques, the protection or countermeasures applied, and the communication channels involved. A first prototype of the playing surface and maps is shown in figure 2.

Fig. 2 Prototype: Social Engineering Theater "Sketch" (in German)

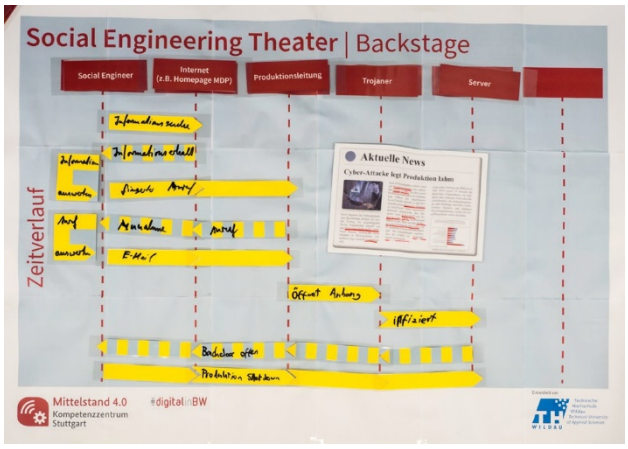

Fig. 3 Prototype: Social Engineering Theater "Backstage"

The second act of the learning scenario, SET "Direction," which is conceived as a digital video quiz, shows individual scenes of various social engineering attacks, on the basis of which the participants have to decide on a course of action.

Subsequently, the participants put themselves in the shoes of a social engineer for the third act, SET "Backstage." Using a fictional newspaper report, they are to reconstruct the attack by connecting the various actors, objects, and activities over time. Figure 3 shows a possible result.

Risk Roulette

This complex learning scenario consists of five steps. First of all, there is a briefing in which the game material and the rules are briefly explained. In the first step, the participants introduce themselves and identify the initial risk. Risk assessment is carried out in the second step, in which the risk category is determined using a 4 × 4 risk matrix based on the frequency of occurrence and potential damage as per [23]. In the third step, the participants must decide on an option for addressing the risk, for which appropriate measures are selected in step four. In step five a decision is made as to whether and to what extent an actual incident occurs on the basis of a certain risk.

Fig. 4 Prototype: Risk Roulette

The Final Testing

The on-site tests with the trainees and students proved to be difficult owing to the distancing rules. Although it was not possible to test with the actual target groups, there were helpful suggestions for improvements.

The online workshops planned for January 2021 will provide insights for further development as well as for the implementation of interactive online events. Afterwards, the final version will be created in each case for both analog learning scenarios and handed over to the client.

4. DISCUSSION, CONCLUSIONS, AND OUTLOOK

Since the two surveys prior to the development process served only to establish priorities, the small number of participants is a limiting factor in our mini project, albeit a negligible one.

Starting out with the preliminary ideas, the development process takes an iterative approach, running through the three phases of prototyping, testing, and adaptation. Testing analog prototypes in times of the COVID-19 pandemic is a special challenge, because the use of digital tools and the development of interactive online formats turned out to be mandatory. This change requires thorough testing with regard to functionality and data protection aspects.

Even though it is generally advantageous to involve the target group in testing the prototypes, the tests with the trainees and students at least yielded sufficient findings to improve the game mechanics and some content details.

Theoretically, a further development iteration would have to take place after testing the learning scenarios with the respective target groups. In practice, the COVID-19 pandemic is a barrier for analog serious games, the financial budget is very limited for the small one-year project, and the project duration is too short for in-depth research.

Since analog formats are not transferable 1:1 into digital ones, a hybrid format is an appropriate alternative, but this is not an exact substitute as the transmission technology and other components are susceptible to interference and the perception channels are limited. In principle, an analog workshop is preferable to a digital workshop because participants have a greater degree of involvement and interact more.

However, more research is needed to find out how well analog GBL scenarios come across in the digital format and to what extent they can be tangibly designed using "hybrid" combinations of analog games and digital transmission. Appropriate equipment is required to ensure good or very good picture and sound quality, and this must

also be thoroughly tested in advance.

We argue that analog GBL scenarios can help to raise awareness among employees about complex IS issues. Further research projects are needed to test this out by developing methods for measuring ISA explicitly.

The experience gained in this project will be incorporated into the next three-year project *Awareness Lab SMEs (ALARM) Information Security*, which has been running since October 1, 2020. In this larger project, on-site attacks are to be carried out and methods for measuring the effectiveness of awareness measures will be developed.

Our experience from other projects with other target groups make it clear that—and this also applies to SMEs—knowledge transfer in awareness-raising measures requires emotional identification and interactive involvement of the participants. The complexity of the specific IS topic must be reduced in order to make the game playable and understandable. In addition, the importance of the topic in everyday situations and workplaces should be made clear through moderation and active discussion.

5. ACKNOWLEDGEMENTS

We would like to thank Dietmar Pokoyski (known_sense) for his imaginative support as an independent contractor in our projects. We thank Simon Cowper for his detailed peer-editing of this paper.

6. REFERENCES

[1] H. Schmidt, J. Gondolf, and P. Haufs-Brusberg, "Studie zur Information Security Awareness in kleinen und mittleren Unternehmen (KMU)", Hochschule Düsseldorf, Medien, Düsseldorf, 2018. doi:10.20385/2625-3690/2018.1

[2] A. Hillebrand, A. Niederprüm, S. Schäfer, S. Thiele, and I. Henseler-Unger, "WIK Report. Aktuelle Lage der IT-Sicherheit in KMU", WIKI Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, Bad Honnef, 2017.

[3] C. Marmulla, "Security für KMU - In 12 Schritten zur Informationssicherheit" in: **computerwoche online**, 2020, retrieved from https://www.computerwoche.de/a/ in-12-schritten-zur-informationssicherheit,3547543. Accessed: December 5, 2020.

[4] K. Aytes and C. Terry, "Computer security and risky computing practices: A rational choice perspective", **Journal of Organizational and End User Computing**, Vol. 16, 2004, pp. 22-40.

[5] A. Tsohou, M. Karyda, S. Kokalakis, and E. Kiountouzi, "Analyzing trajectories of information security awaren- ess", **Information Technology & People**, Vol. 25, 2012, pp. 327-352.

[6] G. Stewart and D. Lacey, "Death by a thousand facts: Cri- ticising the technocratic approach to information security awareness", **Information Management & Computer Security**, Vol. 20, 2012, pp. 29-38.

[7] I. Kirlappos, A. Beautement, and M. A. Sasse, "Comply or die' is dead: Long live security-aware principal agents", in Adams, A.A., Brenner, M. and Smith, M. (Ed.), Financial Cryptography and Data Security, **Lecture Notes in Computer Science**, Heidelberg: Springer, Vol. 7862, 2013, pp. 70-82.

[8] T. Fagade and T. Tryfonas, "Security by compliance? A study of insider threat implications for Nigerian banks". In T. Tryfonas (ed.), Human Aspects of Information Security, Privacy, and Trust, HAS 2016, **Lecture Notes in Computer Science**, Cham: Springer, Vol. 9750, 2016, pp. 128-139.

[9] M. Helisch and D. Pokoyski (Ed.), **Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung**, Wiesbaden: Vieweg + Teubner, 2009.

[10] B. Khan, K. S. Alghathbar, S. I. Nabi, and M. K. Khan, "Effectiveness of information security awareness methods based on psychological theories", **African Journal of Business Management**, Vol. 5, No. 26, 2011, pp. 10862-10868.

[11] E. Albrechtsen, "A qualitative study of users' view on infor- mation security", **Computers & Security**, Vol. 26, 2007, pp. 276-289.

[12] H. Kruger, L. Drevin, and T. Steyn, T., "Email security awareness: A practical assessment of employee behaviour". In Futcher, L. and Dodge, R. (eds.), **Fifth World Conference on Information Security Education**, IFIP – International Federation for Information Processing. Boston, MA: Springer, Vol. 237, 2007, pp. 33-40.

[13] S. Göbel, "Autorenumgebung für Serious Games-StoryTec: Eine Autorenumgebung und narrative Objekte für personalisierte Serious Games", TU Darmstadt, **Dissertation**, 2017.

[14] Institute Of Play, "Q Design Pack School", 2015, retrieved from http://www.instituteofplay.org/wp-content/uploads/2013/09/IOP_QDesignPack_School_1.0.pdf. Accessed: March 3, 2016.

[15] W. Bösche and F. Kattner, "Fear of (serious) digital

games and game-based learning? Causes, Consequences and a possible countermeasure", **International Journal of Game-Based Learning**, Vol. 1, No. 3, 2011, pp. 1–15.

[16] S. Vandercruysse and J. Elen, "Towards a Game-Based Learning Instructional Design Model Focusing on Integration". In Pieter Wouters and Herre van Oostendorp (eds.), **Instructional Techniques to Facilitate Learning and Motivation of Serious Games**. Cham: Springer International Publishing, 2017, pp. 17–35.

[17] D. de Zafra, S. Pitcher, J. Tressler, and J. Ippolito, "Information Technology Security Training Requirements: A Role and Performance-Based Model". National Institute of Standards and Technology (ed.), Gaithersburg, 1998, retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf. Accessed: December 5, 2020.

[18] H. K. Mandal, "Brainstorming Approach And Mind Map- ping In Synergy Creating Activity", **Global Journal of Finance and Management**, Vol. 6, No. 4, 2014, pp. 333– 338, retrieved from https://www.ripublication.com/gjfm-spl/gjfmv6n4_07.pdf. Accessed: December 5, 2020.

[19] S. M. Albladi and G. R. S. Weir, "User characteristics that influence judgment of social engineering attacks in social networks", **Human-centric Computing and Information Sciences**, Vol. 8, No. 1, 2018, DOI: 10.1186/s13673- 018-0128-7.

[20] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework," **Information Security for South Africa** (ISSA), Johannesburg, South Africa, IEEE, 2014, pp. 1–9.

[21] S. Schumacher, "Die psychologischen Grundlagen des Social Engineerings", **Magdeburger Journal zur Sicherheitsforschung**, Vol. 1, 2011, pp. 1–26.

[22] K. D. Mitnick and W. L. Simon, **The art of deception–controlling the human element of securety**, Indianapolis, Ind.: Wiley Pub, 2002.

[23] Bundesamt für Sicherheit in der Informationstechnik (BSI), "BSI-Standard 200-3 - Risikoanalyse auf der Basis von IT-Grundschutz", retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompen- dium/standard_200_3.pdf?blob=publicationFile&v=7. Accessed: December 5, 2020.

English version: "BSI Standard 200-3 Risk Analysis Based on IT-Grundschutz", October 2017. Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.pdf?__blob=publicationFile&v=2. Accessed: July 2, 2020.

[24] bitkom, Spionage, Sabotage und Datendiebstahl– Wirtschaftsschutz in der vernetzten Welt: Studienbericht 2020, Berlin, retrieved from https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschafts-schutz_2020_final.pdf. Accessed: October 14, 2020.

[25] S. Fenz, J. Heurix, T. Neubauer and F. Pechstein, "Current challenges in information security risk management" in **Information Management & Computer Security**, Vol. 22 No. 5, 2014, pp. 410–430. DOI: 10.1108/IMCS-07-2013- 0053.

[26] Berliner Beauftragte für Datenschutz und Informationsfreiheit, "Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten", 2020, retrieved from https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste. pdf. Accessed: December 5, 2020.

[27] M. Kerres, "Frustration in Videokonferenzen vermeiden: Limitation einer Technik und Folgerung für videobasierte Lehren". In K. Wilbers (ed.), **Handbuch Learning**, Köln: Wolters Kluwer, 2020, preprint.