Conducting Interactive Activities to Enhance the Information Security Culture of the Organisation's Staff

Yuriy V. Golchevskiy[a] and Natalia R. Oleneva[b]

Institute of Exact Sciences and Information Technologies, Pitirim Sorokin Syktyvkar State University, Oktyabrsky ave., Syktyvkar, Russian Federation

yurygol@gmail.com, kib@syktsu.ru

Keywords: Information Security Management, Information Security Culture, Information Security Training, Compliance with Information Security Rules and Protocols.

Abstract: Social engineering is one of the most common threats to the information security of commercial firms, government and other organisations. Various technical and administrative protection mechanisms can be applied to reduce the risks associated with social engineering. This paper proposes an approach to designing measures to improve information security culture based on employee training and behavioural monitoring. Employees in the financial and IT sectors were tested using the proposed framework. Training and subsequent series of coordinated test attacks were used to simulate the actual activities of the attackers and monitor the employees' reactions to them. From the test results, it was concluded that the employees tested had a high level of awareness of the attackers' methods and were critical of the information they received. Vulnerable employees were identified who needed additional training and improved information security related skills. In this way, potential threats to user data were identified to be serious, and staff were shown to be more convinced that they must apply the rules and adhere to the organisation's information security policy in their day-to-day practices. Subsequent sharing of experiences and collective reflection, combined with the use of incentives, did have a noticeable impact on information security compliance intentions.

1 INTRODUCTION

In the context of the growing influence of the digital economy adherence to information security rules, policies and standards is critical to protecting valuable corporate information for companies and organisations. The consequences of violating these rules are enormous financial and reputational losses. There is a wide variety of technical, software and hardware security solutions available. However, all of them can be almost useless in preventing information security incidents if the organization's personnel do not follow the protocols for their use. The majority of successful attacks on corporate IT infrastructure exploit the human factor, as evidenced by reports from reputable cybersecurity companies InfoWatch (InfoWatch, 2019), Trend Micro (Trend Micro, 2020) and others. Many malicious programs work in such a way that to launch them, the user has to perform certain actions: open a document sent by email, click a malicious link, etc., which often means departing from well-known cybersecurity rules.

Positive Technologies reports cite statistics showing that cyber-attacks often target government organizations, as well as banks and online services. According to data published by the Bank of Russia Center for Monitoring and Responding to Computer Attacks in the Financial Industry, common crimes in the financial industry include employee email hacking, social engineering techniques, unauthorized access to company data, compromised credentials, exploitation of software vulnerabilities and web vulnerabilities.

The success of this type of attack is often due to reasons such as:

- Lack of or insufficient understanding of information security principles and protocols;
- Carelessness or absent-mindedness in handling corporate information;
- A variety of reasons for employee vigilance, such as opening emails from dubious sources;

[a] https://orcid.org/0000-0003-2047-9138
[b] https://orcid.org/0009-0003-8969-7368

- Perpetrators using new social engineering techniques and improved methods for delivering malware downloaders;
- Insufficient vigilance or equipment of information security officers.

As a result, perpetrators are able to carry out their actions for long periods without being detected. It is evident that there are many causes that are driven by the behaviour of an organisation's employees, which raises the question for its management “What causes this behaviour and what can be done to reduce the risks caused by non-compliant employee behaviour?”

This article explores how, in practice, an organisation can increase employee accountability and awareness of the need for information security compliance by designing an approach to organising training and monitoring of employee compliance with information security rules. The proposed approach have been tested in the activities of organisations operating in the IT services and credit-financial sectors of activity.

2 RELATED WORKS

In the late 1990s, a concept called “information security culture” emerged, closely intertwined with organisational culture. It implied a measure to encourage employees to behave appropriately in the face of emerging information threats and to follow information security norms.

For example, Connolly, Lang, and Tygar (Connolly, Lang, and Tygar, 2014) proposed the conceptualisation of information security culture. Alnatheer (Alnatheer, 2015) presented a study of critical success factors for information security culture, in which he showed that the most important factors are support from senior management for information security, creation of effective information security policy, awareness raising and training, information security compliance, and ethical conduct policy and organizational culture. Soomro, Shah and Ahmed (Soomro, Shah, and Ahmed, 2016) reached the same view based on a systematic review of the literature related to the role of management in information security, further emphasising that organisations need a more holistic approach to information security and suggesting ways in which managers can play an effective role in ensuring it.

Research results cited in (Batmetan, Kembuan, 2024; Tejay, Mohammed, 2023; Choi, Park, and Kang, 2024) suggest that information security knowledge sharing, collaboration, collective reflection, practical experience, response efficiency, self-efficacy, informal work practices and subjective norms have a significant impact on information security compliance behavioural intentions. Sekulla et al. (Sekulla et al., 2020) proposes a tool for knowledge sharing between organisations and the accumulation of experience.

The significant impact of organisational culture based on collaboration, innovation, consistency and efficiency on information security culture is presented in (Alhogail, 2015). It is shown that its change has a significant impact on the ability to address key information security challenges. It is noted that organizational culture has a significant impact on confidentiality and integrity, but not on the availability of information.

Thus, the general message of many works is that more attention should be paid to the behavioural viewpoints of users in relation to information security.

Of course, researchers could not avoid the issue of measuring an organization’s information security culture. In (Rohan et al., 2023; Tang, Li, and Zhang, 2016) the authors discuss management ideas related to how to measure the information security culture of an organization and subsequently determine which viewpoints are important to the organization, as well as evaluation approaches for further implementation and improvement of such culture.

Many works identify and focus on factors that provoke unfavourable employee behaviour in organisations, e.g. Connolly et al. (Connolly, Lang, and Tygar, 2014). At the same time, researchers focus on the existence of a conflict of values between information security and other organizational values, which is often the cause of security non-compliance among employees (Karlsson, Denk, and Åström, 2018).

A significant proportion of researches is motivation researches. Deterrence theory, which is widely used in behavioural information security research, suggests that controls can serve as deterrence mechanisms, increasing the importance of the threat of punishment for non-compliance with information security rules. The paradigm proposed in (Siponen, Adam Mahmood, and Pahnila, 2014) combines elements of defence motivation theory, motivated action theory and cognitive evaluation theory. The authors show that the perception of the severity of potential threats to information security, the belief that employees should apply the established rules and adhere to the information security policy, and the social norms of compliance with this policy have a significant positive impact on the actual compliance of employees with the established rules and policies of information security. In (Connolly, Lang, and Tygar, 2015) the influence of a combination of security countermeasures and cultural factors on employee security behaviour is investigated, and in (Liu, Zhang, and Zhang, 2020) it is argued that informal social control and self-control are more likely to be effective in enforcing security compliance than formal control, and in addition, the influence of formal and informal control on security compliance is also partly due to traditional cultural characteristics. Organisations often use methods to reward and/or punish employees in order to reduce risky behaviour. The authors of the study presented in (Blythe, Gray, and Collins, 2020) investigated how organizations use these methods and what factors influence the use of rewards or punishments (sanctions). It was noted that sanctions are used in 90% of organisations.

The study of the problems associated with the audit of employee behaviour is the topic of (Vroom, von Solms, 2004). It demonstrates that the human behaviour audit procedure is quite complex and therefore, alternative methods should be used where observation of the employee is not necessary. Instead, a more informal approach is proposed to improve the information culture.

D’Arcy, Hovav and Galletta (D’Arcy, Hovav and Galletta 2009) shows that three aspects deter information system misuse: user awareness of security policies, training programs and computer monitoring, and that the perceived severity of sanctions is more effective than the certainty of sanctions.

In the context of the rapidly increasing importance of digital technologies considerable attention is also paid to discussions on the importance, applicability and effectiveness of security training methods. As an example, the following works can be cited (Alyami et al., 2024; McIlwraith, 2021; Kweon et al., 2021). The studies sheds light on the role of security training and education. T. Gundu emphasizes the importance of continuous learning as the cornerstone of cybersecurity culture, presenting cybersecurity culture model that encapsulates the principles of "Learn, Unlearn, and Relearn" as a strategic stance (Gundu T., 2024).

Additionally, it should be noted that many organisations allow employees to use their own personal equipment (e.g. mobile devices) to access corporate networks and data (a phenomenon referred to as “Bring Your Own Device” – BYOD). However, while the technical aspects of BYOD security have been addressed (e.g., papers (Ratchford, Wang, 2019; Zungur et al., 2019)), the information security culture aspects of the BYOD approach remain rather understudied.

In summary, the notion of information security culture is currently a dynamic and evolving one that is being transformed by new realities and research.

3 METHODS

This study is based on empirical research method. The empirical method was applied in the process of approbation of some of the described solutions in the activities of specific organizations, observation and comparison of data obtained in the course of practical approbation of the authors’ activities, as well as interviewing representatives of professional communities for a deeper understanding of the described problem.

The approach presented in this article has been tested at an enterprise providing technical support for the operation of information systems. A service to protect users from phishing attacks (hereinafter referred to as the Service) by reproducing the actions of potential attackers was developed and implemented. More than 1.5 thousand users participated in the study.

The functional feature of the developed Service was the possibility to conduct a simulated attack on users that consisted of sending prepared emails with elements of social engineering that resembled typical emails from attackers but had no destructive functions. The simulations were divided into two types: those with links to a fake website that required input, and those with malicious attachments.

The user actions (simulation results) after receiving the email were divided into three options: neutral, failure and success.

If there was no response from the user, then this result was marked as neutral and was considered close to unwanted, because the goal of the Service was not only to reduce the number of failed online attacks, but also to increase vigilance, e.g. the number of emails sent by users to be checked. Therefore, with this result, the user is reminded to send suspicious emails for verification and the rules for secure handling of emails.

A failure was defined as launching a malicious attachment from an email or entering the requested data on a fake website. In this case, the user was notified of the failure by an email containing a description of the user's error and secure email practices.

A success meant that the user did not launch the malicious attachment or enter the requested data and sent the email itself for verification.

The second type of simulation was far more likely to fail because the user had to do less (click a link, enter data on the site). Running an attachment was more suspicious.

4 RESULTS AND DISCUSSION

Creating a culture of information security in organisations influences employees' security perceptions and behaviour in ways that can protect against many of the information security threats posed by insiders.

But how do you create such a culture in an organisation? The sources studied suggest several approaches to enhancing information security culture, among which are:

- Learning;
- Play methods;
- Motivational methods (both rewarding and punitive methods).

In our opinion, training staff based on lectures alone is not always effective enough, as it can be difficult to absorb the material and subsequently link it to a particular threat with this approach. There are now other ways of training. One example is Riskio, a cybersecurity awareness board game for people without a technical background. Riskio provides an active learning environment where players accumulate knowledge about cybersecurity, attacks and defence, playing both the role of attacker and defender of an organisation's critical assets (Hart et al., 2020).

Despite the challenges of conducting employee behavioural audits noted earlier, we consider them a crucial part of the ongoing effort to improve an organisation's information security.

The use of interactive techniques, such as mock attacks on users, can be an effective method. With this approach, the user can "feel" the effects of the attack (hardware failure, data theft and blockage, etc.) Hacker attack simulation allows you to identify your most vulnerable employees and give them extra training. That is, the knowledge and skills acquired during training must be accompanied and reinforced by practical verification of employees' compliance with information security rules in the organization.

Consider the stages of implementing such an interactive methodology, described using the SADT diagram shown in Figure 1.

Four stages can be distinguished:

1. Definition of the main objectives;
2. Testing: initial and re-testing, which takes place after the training phase;
3. Training - a stage in which staff (users) at risk are trained and tested;
4. Testing of system effectiveness – evaluation of how useful and effective the methodology used was.

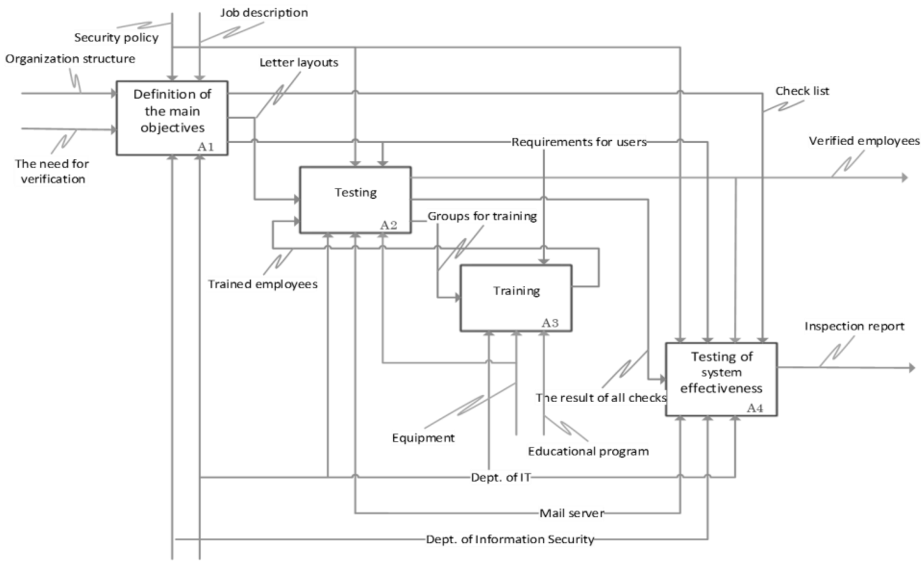

Figure 1: SADT diagram presenting the stages of the approach to implementing an information security compliance check for company employees.

Let us consider each stage in more detail.

A1 – The goal setting stage, where the scope and extent of the audit, the requirements to be checked, and the timeframe for the audit are defined. Based on this information, a checklist for verification is drawn up.

A2 – Verification of employees. A simulated attack is performed (e.g., sending out a trap email according to the focus groups defined in the first step), followed by the collection and analysis of statistics on insecure behavior (e.g., clicking links, opening attachments, etc.).

Once the data is systematised, employees who have made mistakes are divided into training groups and additional training is provided to them (Block A3). This scheme can be applied more than once for repeated checks. The results of the checks will form the basis for the last stage.

A4 – Check the effectiveness of the system. A checklist check is carried out in this final stage:

- The status of each item for all selected divisions in the organisational structure of the company or organisation (divisions, departments etc.) is determined;
- The results of the check are recorded.

After this, it is possible to proceed to:

- Formulation of proposals for the elimination of deficiencies;
- Formulate a plan to eliminate them;
- Conduct an analysis of the necessary costs and capabilities of the organisation to eliminate and prevent re-occurrence of incidents.

Decomposition of stage A4 shown in Figure 2.

A report can be generated at the end of the verification, including the results obtained in step A2 “Verification”, a checklist evaluation and a plan of recommended actions.

In the event that a company decides to carry out such an audit in-house, it will be necessary to:

- Draw up a list of mailboxes and users to whom the test letter will be sent.
- Create a web resource that is set up to monitor requests and keep a personalised record of visitors. In addition to this, the user is informed of a test infection of their computer by malicious code that they need to report to their manager.
- Prepare a test file that will take the user to the web resource described above.
- Register e-mail addresses on various mailing resources to organise a mailing list.
- Determine the type of messages to be sent. The messages should be relevant to the activity profile of the employees being tested.

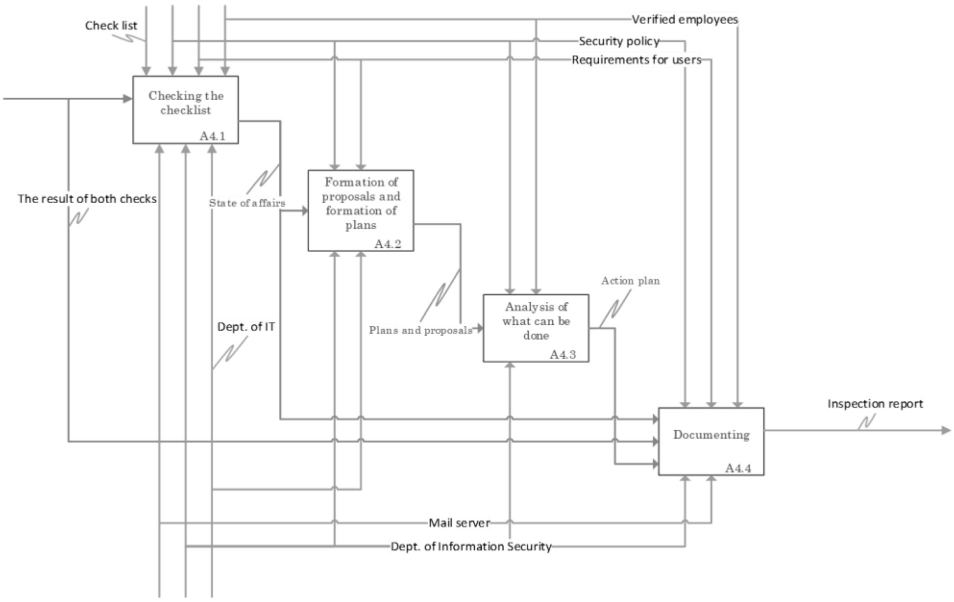

Figure 2: SADT diagram presenting the decomposition of stage A4 “Testing of system effectiveness”.

During the piloting of the Service, feedback was maintained with the users: phone calls, emails, text reports etc. to evaluate the functioning of the Service, the possibility of further analysis of the situation and staff attitudes towards issues related to the formation of secure behaviour. In the first two months of the trial, there were a large number of complaints from users that they received simulations too often (every six months to a month) and that this distracted them from their duties.

This problem was solved by creating a Service function that would take into account users' proven skills and knowledge and regulate the frequency of receiving simulations depending on them.

To this end, the concept of “competence” was introduced. A competence is an electronic mark indicating the possession of certain skills and knowledge in the field of information security.

However, we would like to point out that in general the use of the Service did not provoke any strong negative reactions from employees.

The main purpose of testing the tool was to increase the security culture of the users and hence reduce the number of failed simulations.

The Service was piloted over a five-month period. Over five months the number of failed simulation emails with a link to a fake website decreased by around 19%, the average number of simulation emails with a malicious attachment decreased by 11%, and the number of simulation emails sent for review increased by more than 30%, as shown in Figure 3 and Figure 4.

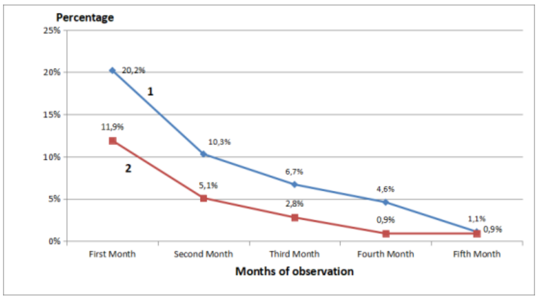

Figure 3: Graph of changes in the number of failed simulations (1 – Simulations with links, 2 – Simulations with attachments).

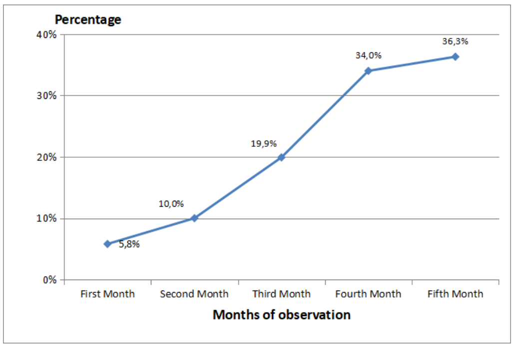

Figure 4: Graph of changes in the number of letters sent by employees for additional checking.

When a similar methodology was tested in an organisation operating in the financial services industry, similar results were obtained, with a difference in quantitative indicators, largely due to the smaller number of employees involved in the piloting.

Studies were conducted with both employees using corporate equipment and those using their own equipment (BYOD). It was noted that the second group had a more serious attitude towards compliance.

5 CONCLUSIONS

Social engineering is one of the most common threats to the information security of commercial firms, government and other organisations. Various technical and administrative protection mechanisms can be applied to mitigate the risks associated with its use.

The proposed scheme was used to test and train employees of financial and IT organisations. Training and a subsequent series of coordinated test attacks were used to simulate actual attacker activity and track employee reactions to them. Harmless files were used to send out email messages and only the launch was recorded during the test.

From the test results it was concluded that the tested employees had a high level of awareness of the attackers’ methods, were critical about the information they received and could detect a phishing email for example, that is they paid attention to the sender details, the subject of the email, logos and names (the emails used company logos and name-calling), links in the email text, signatures and contact information as well as grammar and spelling mistakes in the text. Vulnerable employees were identified who needed additional training and improved information security-related skills.

Thus demonstrating the seriousness of potential threats to user data, there was a growing conviction among employees that they should apply the established rules and adhere to the information security policy in their day-to-day practice. The ensuing exchange of experience and collective reflection, together with the application of incentives, did have a noticeable impact on information security compliance intentions, shaping some collective norms on the issue.

Overall, such testing in practice proved to be useful for the organisation and was highly appreciated by the organisations’ management.

The importance and usefulness of having management controls and activities in place to help build and maintain an information culture was noted by staff themselves. It was felt, however, that it was more useful to encourage secure behaviour than to punish and sanction risky behaviour.

In our view, formal management control (i.e. deterrence, reward and monitoring) remains an important part of building and developing an information security culture. Getting it right is one of the most complex, but essential, solutions for ensuring an organisation's information security.

REFERENCES

Alhogail, A., 2015. Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study. International Journal of Security And Its Applications, 9(7), 163–178.

Alyami, A., Sammon, D., Neville, K. and Mahony, C., 2024. Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives. Information and Computer Security, Vol. 32 No. 1, pp. 53-73.

Alnatheer, M. A., 2015. Information security culture critical success factors. Proceedings – 12th International Conference on Information Technology: New Generations, ITNG 2015, 731–735.

Batmetan, J. R., Kembuan, D. R. E., 2024. Effects of Knowledge Sharing Methods on Cyber Security Practice in Small Medium Enterprises'. Proceedings of the 5th Vocational Education International Conference (VEIC-5 2023), Advances in Social Science, Education and Humanities Research 813, Atlantis Press, pp. 28 – 37.

Blythe, J. M., Gray, A., Collins, E., 2020. Human cyber risk management by security awareness professionals: Carrots or sticks to drive behaviour change? Lecture Notes in Computer Science, Vol. 12210, 76–91.

Choi, H., Park, S., and Kang, J., 2024. Enhancing Participatory Security Culture in Public Institutions: An Analysis of Organizational Employees' Security Threat Recognition Processes. IEEE Access.

Connolly, L., Lang, M., Tygar, D., 2014. Managing employee security behaviour in organisations: The role of cultural factors and individual values. IFIP Advances in Information and Communication Technology, 428, 417–430.

Connolly, L., Lang, M., Tygar, J. D., 2015. Investigation of employee security behaviour: A grounded theory approach. IFIP Advances in Information and Communication Technology, 455, 283–296.

D'Arcy, J., Hovav, A., Galletta, D., 2009. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79–98.

Gundu T., 2024. Learn, Unlearn and Relearn: Adaptive Cybersecurity Culture Model. Proceedings of The 19th International Conference on Cyber Warfare and Security, 95-102.

Gurvirender P. S. Tejay, Zareef A. Mohammed, 2023. Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. Information & Management, Vol. 60, Issue 3, 103751.

Hart, S., Margheri, A., Paci, F., Sassone, V., 2020. Riskio: A Serious Game for Cyber Security Awareness and Education. Computers and Security, 95.

InfoWatch, 2019. Data Leakage News. Available at: https://infowatch.com/analytics/leaks_monitoring Accessed 4 Apr 2024

Karlsson, M., Denk, T. and Åström, J., 2018. Perceptions of organizational culture and value conflicts in information security management. Information and Computer Security, 26(2), 213–229.

Kweon, E., Lee, H., Chai, S. et al., 2021. The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. Information Systems Frontiers, Vol. 23, 361–373.

Liu, J., Zhang, J., Zhang, J., 2020. Validating a control-based model of information security policy compliance – A meta-analysis. 40th International Conference on Information Systems, ICIS 2019. Munich, Germany

McIlwraith, A., 2021. Information Security and Employee Behaviour. How to Reduce Risk Through Employee Education, Training and Awareness. Routledge. London, 2nd Edition.

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., and Thapliyal, H., 2023. A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon, 9(3). Available at: https://www.cell.com/heliyon/pdf/S2405-8440(23)01441-X.pdf Accessed 4 Apr 2024

Ratchford, M. M., Wang, Y., 2019. BYOD-Insure: a Security Assessment Model For Enterprise BYOD. 5th International Conference on Mobile and Secure Services, MobiSecServ 2019, 1–10. Miami, United States. Sekulla, A., Giatagantzidis, J., Dax, J., Pipek, V., 2020. A lightweight tool for measuring the impact of IT security controls in critical infrastructures. ECSCW 2019 – Proceedings of the 17th European Conference on Computer Supported Cooperative Work. Salzburg, Austria.

Siponen, M., Adam Mahmood, M., Pahnila, S., 2014. Employees' adherence to information security policies: An exploratory field study. Information and Management, 51(2), 217–224.

Soomro, Z.A., Shah, M. H., Ahmed, J., 2016. Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215–225.

Tang, M., Li, M., and Zhang, T., 2016. The impacts of organizational culture on information security culture: a case study. Information Technology & Management, 17, 179–186.

Trend Micro, 2020. Disrupting the Workplace: Trend Micro 2020 Midyear Cybersecurity Report. Availible at: https://documents.trendmicro.com/assets/rpt/rpt-securing-the-pandemic-disrupted-workplace.pdf Accessed 4 Apr 2024

Vroom, C., von Solms, R., 2004. Towards information security behavioural compliance. Computers & Security, 23(3), 191–198.

Zungur, O., Suarez-Tangil, G., Stringhini, G., Egele, M., 2019. BorderPatrol: Securing BYOD using Fine-Grained Contextual Information. Proceedings – 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 460–472.