Security level evaluation with F4SLE

Mari Seeba
University of Tartu
Tartu, Estonia
Information System Authority
Tallinn, Estonia
mari.seeba@ut.ee

Tarmo Oja
University of Tartu
Tartu, Estonia
Cybernetica AS
Tallinn, Estonia
tarmo.oja@ut.ee

Maria Pibilota Murumaa
University of Tartu
Tartu, Estonia
Cybernetica AS
Tallinn, Estonia
maria.pibilota.murumaa@ut.ee

Václav Stupka
Masaryk University
Brno, Czechia
CyberSecurity Hub, z.u.
Brno, Czechia
stupka@muni.cz

ABSTRACT

In the realm of security measurements, extensive efforts have been made to evaluate and compare security levels at the country level, resulting in various indices. However, there has been a dearth of evaluations focusing on the information security posture of individual organizations and simultaneously on state-level status evaluation. Such evaluations hold significant potential for providing valuable feedback on the security status of organizations and facilitating assessments and supportive data-driven focused interventions at a national level. This study leverages the Framework for Security Level Evaluation (F4SLE) and the developed tool, Measurement Application for Self-assessing Security (MASS), to collect data for the evaluation. The paper presents diverse options for interpreting the collected data and establishes the foundation for an ongoing cross-country study. The results encompass the analysis of organization-level data and offer insights into overall approaches to security across organizations. This study is a preliminary step toward a more comprehensive information security examination.

CCS CONCEPTS

• **Security and privacy**;

KEYWORDS

information security level evaluation, F4SLE, maturity of security, NCSC

ACM Reference Format:
Mari Seeba, Tarmo Oja, Maria Pibilota Murumaa, and Václav Stupka. 2023. Security level evaluation with F4SLE. In *The 18th International Conference on Availability, Reliability andSecurity (ARES 2023), August 29-September 1, 2023, Benevento,Italy*. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3600160.3605045

ARES 2023, August 29-September 1, 2023, Benevento, Italy

ACM ISBN 979-8-4007-0772-8/23/08.
https://doi.org/10.1145/3600160.3605045

ACKNOWLEDGMENTS

This work is part of the Cyber-security Excellence Hub in Estonia and South Moravia (CHESS) project funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

1 INTRODUCTION

Any measurement shall aim at reducing uncertainty. Measuring or evaluating the security levels of an organization allows the creation of an appropriate protection strategy by reducing ignorance by implementing security measures to prevent potential damage. For example, the ENISA Threat Landscape Report[1] names the TOP 8 threats (ransomware, malware, social engineering threats, threats against data, threats against availability [Denial of Service], threats against availability [Internet threats]), disinformation – misinformation, supply-chain attacks). They are threats to every organization but can also affect the national situation.

Also, to ensure the security and privacy of Intelligent Infrastructures (II), it is necessary to implement an organization-wide information security management system.

The organization may, for example, establish compliance with the recommendations offered by the country or with some of the best practices (e.g., ISO27001 or NIST Cybersecurity Framework standards). In this case, information about the organization's security will remain available only to a specific organization. It would be necessary to collect data on security at the national level with the same instrument to create a national strategy based on relevant data.

Such studies have been carried out at the national level, but only a few have reached scientific publications. An example is Poland [12], where the security evaluation was performed for four years (2016-2019). The findings indicate a notable and positive impact resulting from the enforcement of GDPR. Another key observation was that business administrators are aware of the protection requirements

(i.e., regulations and contracts), and the IT management is knowledgeable about security measures, but due to a lack of communication, the business and technical sides are not aligned. Also is not clear how the organizations got their individual security status assessment results.

Hasan et al. [3] found a significant positive correlation between adherence to cyber security standards and higher readiness in organizations to combat cyberattacks in Bahrain. Also, if the research covers only one state, the different approaches to security management are not systematically studied.

A number of literature reviews describe several security assessment frameworks, maturity evaluation models, or security assessment methods [5, 6, 8]. But there is no mentioning of dual proposed use at the organization level and simultaneously on the state level or over organizations.

In Estonia, a thorough information security measuring and comparison has not been conducted before. We developed a framework with updateable content for security level evaluation called F4SLE [10, 11]. The content of F4SLE encompasses security measures for both the II itself and the organization's overall information security management system. It was used in a small group of organizations to provide self-assessment and cross-organization comparison during the implementation of the Estonian Information Security Standard (E-ITS) [9]. The pilot was the first time that F4SLE was used. A wider evaluation and deeper analysis of the results are yet to be conducted.

The objective of this work is to answer the following questions:
RQ: What are the avenues for interpreting the data collected using the security evaluation instrument F4SLE?

Answering the questions is the intermediate result and input for ongoing data collection project. The data collected for this work is based on both Estonian and the Czech Republic organizations' input. In this article we give an overview of the conduct of the study, the instrumentation, and the results interpretation options based on preliminary data analysis.

2 BACKGROUND

The terms measurement, assessment, and evaluation are often used interchangeably in the field of security. However, they have distinct meanings and purposes [4]. Measurement involves quantifying attributes or characteristics to obtain standardized numerical results. On the other hand, assessment focuses on gathering information in a specific area to provide feedback and gain a deeper understanding of issues, such as identifying risks. Evaluation consist collecting and analyzing data to judge the extent to which goals (security maturity levels) have been achieved. For security evaluation, we used F4SLE as the framework and content. We developed the MASS tool to simplify the use of F4SLE and data collection for further analysis and benchmarks.

2.1 F4SLE

F4SLE [11] is an instrument for evaluating organization security maturity level. F4SLE is based on the Estonian Information Security Standard E-ITS [9]. F4SLE enables respondents to evaluate security in ten security dimensions (see descriptions of the dimensions in Table 1).

Table 1: Security dimensions of F4SLE

Dimension	Description
ISMS	Organisation's information security management system, incl: management involvement, responsibilities distribution, asset, and resource management.
CON	Concepts and guidelines, incl: backups, archiving, development, personal data protection, cryptography, awareness, and data exchange agreements.
ORP	Information security management, incl: IT usage policies, personnel policy, identity and access rights management, and training.
OPS	IT operations management and documentation: specific hardware, software, network components, cloud services, and remote work.
DER	Incident handling, IT forensics, audits, exercises, and emergency preparedness.
IND	Industrial IT systems, incl: machine control computers, sensors, robots, lab and diagnostic equipment, and warehouse systems.
NET	Network component management.
INF	Infrastructure like buildings, rooms, cabling, mobile workplaces, vehicle IT solutions, and smart houses.
APP	Application software, groupware, directory services, and subscription software management, including updates and logging.
SYS	Systems and hardware, incl: servers, computers, tablets, phones, removable media, and virtualization solutions.

The levels of each dimension are inherited from the E-ITS levels (Basic and Standard), and each dimension level consists of at least one attribute. In F4SLE, the Basic level is divided into three: *initial*, which covers the awareness of security needs; *defined*, covering documentation requirements; and *basic* comprising practical issues. The *standard* level corresponds to sustainability, monitoring, and the capability to react to unknown risks.

The respondent should evaluate each dimension attribute, altogether around 200 attributes [10]. Attributes should be evaluated on the four-level scale (implemented (scoring 3), implemented with minor shortcomings (2), partially implemented with significant shortcomings (1), and not implemented (0)). In some cases, the respondent can refuse to respond or indicate that the attribute is not applicable to the organization. Due to E-ITS and the threat landscape changes, the attributes are updated yearly.

After responding to the attributes, aggregated results are calculated (each level average per dimension and levels average per dimension) and presented. Results are provided for each dimension in the scale of 0.0..3.0.

F4SLE does not impose any prerequisites on organizations for evaluating their security level in order to maintain a low entrance barrier.

2.2 MASS

The Measurement Application for Self-assessing Security (MASS) serves the purpose of presenting the F4SLE to respondents, providing immediate results on the organization's security status after responding to all security attributes, and collecting averaged results for cross-organizational analysis. MASS is built as a client-side JavaScript application running in a web browser. Using the tool, a respondent can select the most applicable evaluation for each F4SLE attribute. For an overview of the answer, choices are color-encoded.

Respondent evaluations are not submitted to the server nor stored in the browser cache, the computations for the result calculations are done on the client side. Average values per dimension per level are submitted to the server if the respondent gives explicit consent and fills in the required meta-data (e.g., name, size, domain; see Table 2) about the respondent organization. If answers are submitted, evaluation results are visualized and described.

MASS provides an opportunity to compare the organization's results to the provided benchmarks (prepared by the F4SLE analyst). Benchmarks can involve yearly and include domain-specific average results. To provide long-term comparability of the results, the respondent has the option to save their responses to their own computer and re-evaluate results later using updated benchmarks.

3 F4SLE APPLICATION

Our empirical study employs a survey approach to gather data on organizations' information security management systems. The survey method, described in [13], is used for experimentation.

Target group. The primary target group was the pilot group of E-ITS implementers, consisting of five municipalities, two hospitals, one non-profit organization, and some public sector institutions. However, as more organizations were interested in evaluating the level of security, we expanded the target group to include schools and private companies and invited universities to participate. Thus, we formulated the target group as organizations whose services depend on information technology and which are obliged to implement information security measures due to regulations.

Instrumentation. To facilitate data collection, we utilized the MASS tool and F4SLE as the tool's content of the survey (see Sec. 2). Participants were provided with a public link to the MASS tool[1], where they evaluated their organization's information security situation based on F4SLE attributes. Using a four-point scale, respondents indicated the level of implementation for each attribute (fully implemented, implemented with some deficiency, implemented with significant shortcomings, not implemented). They also had the option to leave an attribute unanswered or mark it as irrelevant to their organization.

Responses were collected individually and self-paced, allowing participants to pause and resume later if needed. This feature was usable by downloading the responses into the respondent's device. Additionally, respondents could consult with other organization representatives during the pause if necessary.

Once all 189 attributes were answered, the MASS tool generates an evaluation result for the organization, presented in a radar diagram. This diagram depicted the organization's situation on a ten-dimensional scale. Results were provided for each level (initial, defined, basic, standard), as well as a summary result. After uploading their results to the data collection server, participants received available benchmarks for local governments, schools, and the overall average. Only metadata and averaged results for each dimension level were collected to the server and used for subsequent research calculations.

[1] https://mass.cloud.ut.ee/massui/

Table 2: Collected metadata with options

Data type	Options
Domain	Healthcare; Municipality; Government office; Education; ICT; Other private sector; Non-profit; Other (specify)
Workplaces	1...30; 31...100; 101...300; 301...1000; 1001...
Hours	Around 30 minutes; Around 1 hour; 2 hours; 2-4 hours; 4-8 hours; More than 1 working day
Role	IT manager; Information security manager /specialist; Management; Network/system administrator; Administrative assistant/lawyer/DPO ; Other (specify)
Country	Czech Republic; Estonia; Other
Implemented standards	ISO/IEC 27001; ISKE (Estonian); CIS Controls; KüTS (Estonian); NIST CSF; E-ITS (Estonian); BSI IT Grundshutz (German); Act on cyber security, no. 181/2014 Coll. (Czech)

Due to the confidentiality requirements outlined in the Public Information Act of Estonia, individual attribute responses were not collected from the organizations.

Processing. The organization average results with organization meta-data are submitted to the collector server in JSON format. The collector server does preliminary format validity checks and assigns a random identification for each response.

Prior to calculating benchmarks, the analyst will remove invalid (e.g., meta-data is clearly faked) and duplicate (e.g., one organization has submitted multiple times) responses. Calculating benchmarks, domain-specific snapshots, and visuals for the demonstrations are done using Python3/Pandas, developed using Jupyter Notebook.

Metadata set. The Estonian and Czech researchers jointly agreed upon the set of metadata based on previous experience and stakeholders' recommendations (piloting group and National Cyber Security Centre (NCSC)). The regulations and standards of information security management that have been in use so far were separately agreed upon based on the official requirements of the countries participating in the study. Collected metadata with options is described in Table 2. Domains are derived based on the target group. Hours are the spent time to fulfill the MASS.

4 RESULTS

Respondents. 26 of 28 of the organizations participating organizations in the survey were from Estonia. Two Czech organizations were also involved in the study. In this study, due to privacy reasons, we do not consider Czech organizations separately but include them in a complete sample. We agreed with the respondents that only group-based results would be publish if the evaluation results were

from at least five organizations belonging to the corresponding group.

Eleven participating organizations were municipalities. In the educational sector, six general education schools and three universities participated. Also, there were four state institutions and two IT companies; the remaining domains (healthcare, non-profit) were listed once. The workstation's amount and the respondent's role are counted in Table 3.

Table 3: Organizations and respondents characteristics

Workstations	Count	Respondent role	Count
1..30	3	Management	4
31.. 100	9	Security officer/specialist	11
101..300	7	IT manager	8
301.. 1000	5	Lawyer/DPO	1
1001 ..	4	Other IT	4

Based on the collected metadata and the results based on the content of F4SLE, the collected data set allows us to characterize the organization's security status and describe the security status over the organization level.

Individual organization results. Each organization receives its result from MASS after finishing its response. The result provides an assessment of each maturity level separately (see an illustrative example of one organization result in Fig. 1), but also describes the overall level of security risk in the organization (see Fig. 2) with the benchmark of the participating organizations or direct domain. Dimension cover different security features (see Table 1 for descriptions of dimensions).

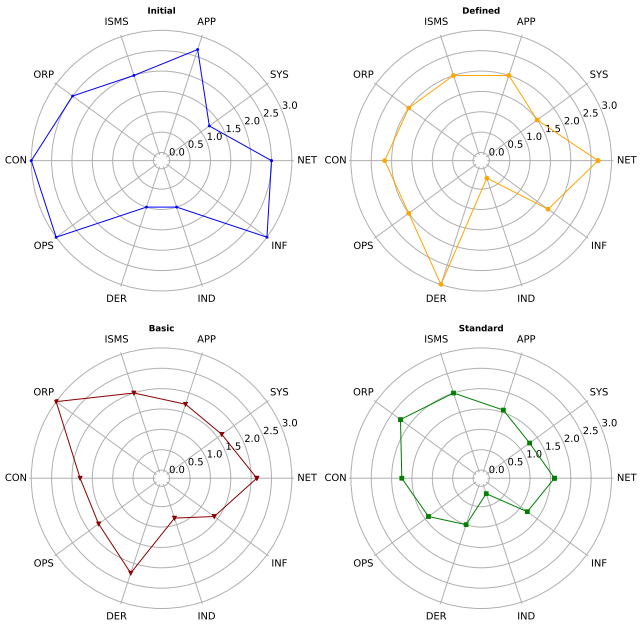


Figure 1: Security evaluation result example of one organization, breakdown by maturity levels

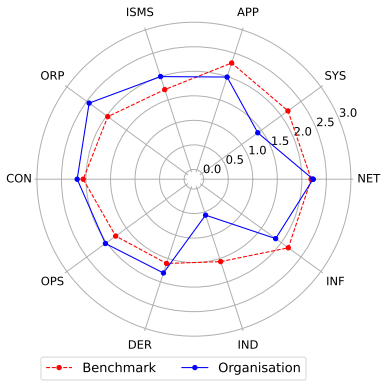


Figure 2: Security evaluation result example of one organization, comparison with the benchmark (cross-organizational average result)

On this basis, the organization can assess its weaknesses and plan information security priorities and activities. Based on the levels, an overview arises of whether the organization has contributed uniformly to both documentation (see Defined level in Fig. 1 in right top) and practical security (see Basic level in Fig. 1 in left down) and how sustainable it is (see Standard level in Fig. 1 in right down). Based on E-ITS, the goal of each organization [9] is to reach the maximum possible result at the Initial, Defined, and Basic levels. All these attributes are mandatory to implement by E-ITS. Also, the organizations should achieve at least partial implementation of the Standard level (scale value > 1). In Fig. 2, the lower the value on the scale, the greater the risk. The goal in an organization that manages risks well should be at least a value of > 2.25 based on the mandatory requirements of the E-ITS standard.

For an illustrative organization example in Fig. 2, we can say that with procedural dimensions (e.g., ORP, CON, OPS), the situation is better than with system dimensions (e.g., SYS and IND). To interpret the IND module, we can say that it is necessary to create an understanding of the applicable automation devices and their configurations and to take appropriate measures. At the moment, it can be assumed (the respondent of the organization knows more about it) that the need to deal with the issues in the security context has not been clearly targeted so far, and responding to the attributes recognized the nature of the problem. However, the weak performance in the DER module indicates a situation where the detection and handling of security incidents require urgent action, as potential risk situations are not even detected. The detailed levels in Fig. 1 provide insight to DER that documentation and concepts (Defined level) are in good shape, but implementing the procedures needs effort. Analyzing by dimensions provides a complete picture of the organization's security status. In conclusion, it can be said that the organization has not yet reached a sustainable level of maturity and can be characterized in each dimension (except DER, IND, and SYS) by "Practices work and are documented, resources are planned, and roles and responsibilities are allocated. Regularity of activities has not yet been achieved".

Cross-organizations results. The information security situation can be characterized by security dimensions across the organizations that participated in the study. Averaged results (e.g., mean and median), which provide one data point per dimension, are suitable for benchmarks (for example, see Fig. 2 or Fig. 5). Scatter areas or distribution of organizations' results better characterize the differences between organizations (see Fig. 3). The collected data can be compared on the basis of metadata (see Table 2) to find relevant correlations (e.g., large organizations vs. small organizations and related trends).

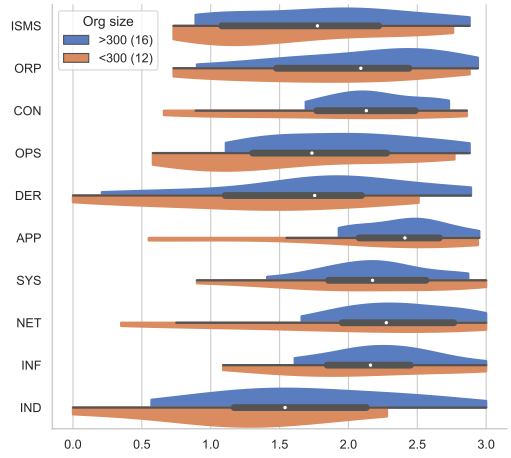
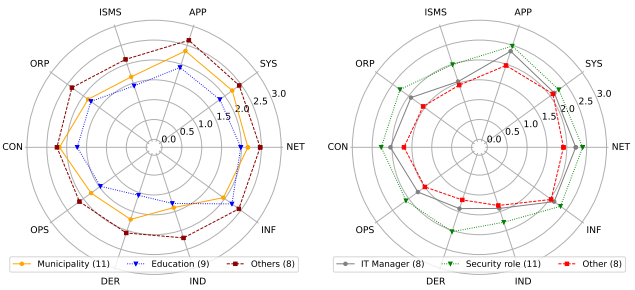


Figure 3: Overall evaluation distribution by dimensions and organization size. The median has been marked with a white dot and 50% by the black thick line.

The results obtained across organizations are used to compare an organization's result with the overall benchmark (e.g., Fig. 2) or other organizations in their domain.

In our early-stage study example, we can characterize the security situation of different domain organizations by dimensions based on the currently collected data (see Fig. 4a). The figure separately visualizes the status of the education sector (general schools) and municipalities. The figure shows that schools' result (blue line) values are lower than the municipalities (yellow line) in all dimensions (except INF). That means when comparing schools and municipalities, the security status is worse at schools. At the same time, it can be seen that schools have contributed to infrastructure and physical security (INF) more than to other dimensions. ISMS, ORP, DER, and IND modules have lower values than other dimensions of municipalities.

For municipalities, central intervention and awareness of the need for management involvement, incident management, and improved access management would be appropriate. However, industrial automation issues have been overlooked in the security requirements so far and now need to be integrated into the security management of institutions. Separately, it is worth noting that the municipality's results of technical modules in the dimensions of APP, SYS, and NET are in a relatively good state, from which it can be concluded that the technical measures have been implemented



(a) By domain **(b) By role**

Figure 4: Overall evaluation result breakdown by (a) organization domain and (b) respondent role.

at a satisfactory level and for them, not all local governments need to be trained separately.

As a result of our survey, which sample is still tiny for convincing results, we can show the results related to respondents' roles separately without violating data privacy (see Fig. 4b). In this regard, it should be mentioned immediately that the organization's size can significantly affect this result. Notably, there are no separate security managers in small institutions, and an IT manager often performs this role. There may not be an independent IT manager in smaller organizations, as the service is outsourced or someone is engaged in IT in addition to their primary work. From Fig. 3, we can see that in smaller organizations, the security situation is generally worse than in large ones – responses from the smaller organizations are shifted to the left, and distribution is greater.

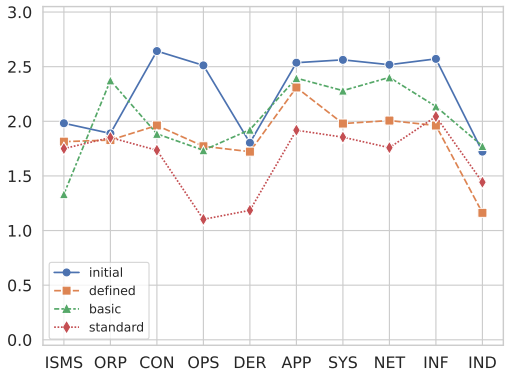


Figure 5: Overall evaluation results by maturity levels

The results also include measurement per each level, as presented in Fig. 5. Reviewing the data reveals that awareness (initial level) is in relatively good shape in six of the dimensions (CON, OPS, APP, SYS, NET, INF) but has clear deficiencies in four (ISMS, ORP, DER, IND). The OPS dimension is well covered with awareness but has a clear deficiency in sustainability/monitoring (standard) level; other levels are in a moderate state. Systematic deficiency can be observed with IND and DER dimensions – all levels are measured low.

5 DISCUSSION

We can draw various conclusions from the overall evaluation results, but the interpretation must be meaningful and supported with background information so it is usable for governing state or EU-level strategies. For example, the NCSC can provide training or supporting materials, organize information campaigns for the target group, and finance relevant projects to improve the situation (e.g., some of these initiatives can be seen here [9]). EU can also alter its policies and initiatives based on domain or international comparative analysis done using MASS within, i.e., the European Cybersecurity Competence Centre (ECCC) network.

For that, we need reliable interpreted data. We cannot conclude from Fig. 4b that only hiring a security manager would improve the security status. The size of the organizations (see Fig. 3) and maturity (see Fig. 5) must also be taken into account when strategies are developed.

The current results show the wide distribution of smaller organizations (see from Fig. 3, <300 workstations) and generally for DER, IND (Fig. 5) topics. Organizations need supportive measures like incident management training and industry automatics security skills. Individual approaches to the low-side outliers should reveal the reasons for low scores in maturity levels.

It must be recognized that each organization has better insight than centrally provided evaluation instrument results into its business requirements and context. A generalized evaluation instrument and benchmarks can support internal processes and development, as illustrated in Fig. 1 and 2, but the organization must do reasoning. For example, why does the documentation of the DER defined level show high values, but awareness of the DER initial level (incident management) is low - this can be explained only by the organization itself.

Evaluation methodology and data collection tools might affect the trustworthiness of the results.[7, 13] The current methodology requires data submission with the organization's name and other parameters. It can be hypothesized that the anonymity of this kind of evaluation might yield more honest results, but for data validation reasons, the organization name provides an invaluable identifier for cross-checking meta-data.

Limitations. The research group could not engage organizations based on a random sample but rather on those reached out to individually. This approach may have limited the study's representativeness, as organizations with lower security awareness may not have been included.

The current results are primarily derived from the respondents dominated by municipalities. As their security posture significantly impacts the overall results and benchmarks, the results are not representing the overall security posture. Therefore the examples presented in this paper are illustrative for the research.

Full statistical data analysis is not yet implemented in this research stage. Defining measurement error and rules for excluding outliers needs to involve a bigger group of respondents.

The results are based on a self-assessment questionnaire, which may lower the study's reliability. Some organizations may overestimate their security posture, while others may lack a complete understanding of their actual situation and rely solely on their gut feeling.

In large organizations (with more than 301 computerized workstations), the correctness of the responses may be reduced by a single person to answer to the attributes alone. This task becomes more challenging when generalizing the status of the workstations and processes within an organization. Respondents may base their answers on policies rather than actual conditions in such cases. If the policies are implemented, the response may reflect the actual status; otherwise, the opposite may be true.

Also, the respondent's role could affect the results based on the role responsibilities and awareness of the security in the organization.

Lastly, since F4SLE is based on the Estonian Information Security Standard, there could be some statistical bias when comparing results between Estonia and other countries.

6 CONCLUSION

The aim of this study was to (**RQ**) provide opportunities for the interpretation of data collected with F4SLE. At the organizational level, F4SLE offers to the respondent

- an evaluation of the organization's maturity levels by security dimensions;
- an aggregated result, which can be interpreted as a risk level (the lower the value, the higher the risk),
- a benchmark to compare organization result with other organizations or domains averaged results.

On the basis of the collected data across organizations the interpretation of data can be based on two principles:

- data dispersion, which characterizes the difference between organizations, and
- aggregated results, such as mean or median, which allow to create a comparison based on individual data points, e.g., compare results over time, provide benchmarks.

Metadata and combinations of metadata (see Table 2) are helpful for interpreting the data, enabling correlations and identifying causal relationships. This study provides only the main directions and is primarily used to motivate further research.

Future Work. Our plan for the near term is to expand the survey by increasing the number of respondents in Estonia and Czechia (South Moravia) and creating new categories of respondents. Our aim is to obtain more reliable results by growing the sample.

We plan to repeat the data collection at least twice to capture the situation's dynamics yearly for the long-term view and comparability. For that, we will update the F4SLE attributes to ensure that they reflect the current threat landscape and that results reflect the actual capabilities.

As one approach, the research group sees an option to compare responses from the same organization but given by different organizational roles. It would enable us to ask how and why persons grasp security aspects within the same environment. This type of study is more relevant for medium and large organizations with role and responsibility separation.

We intend to conduct more data analytics and link it to other databases to establish causal relationships between the description of the situation, such as the threat landscape, events affecting security, and specific regulations.

We plan to involve national decision-makers in the study to assess the possibility of using the results to develop security-related strategies. Collecting the same data from Estonia and the Czech Republic simultaneously will also provide opportunities to study the impact of local and EU regulations and standards in different countries.

For instance, Estonia has a reference security catalog E-ITS [9] that provides standard measures for typical assets alongside risk management measures derived from risk consideration. On the other hand, the Czech Republic follows the ISO/IEC 27001 [2] approach, requiring organizations to derive the risk management measures based on their risks.

REFERENCES

[1] ENISA. 2022. ENISA Threat Landscape 2022. https://doi.org/10.2824/764318

[2] International Organization for Standardization. 2022. ISO/IEC 27001:2022 Information security management systems. Requirements.

[3] Shaikha Hasan, Mazen Ali, Sherah Kurnia, and Ramayah Thurasamy. 2021. Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications* 58 (2021), 102726. https://doi.org/10.1016/j.jisa.2020.102726

[4] W Huitt. 2007. Assessment, measurement, and evaluation: Overview. *Educational Psychology Interactive* (2007).

[5] Mahmoud Khaleghi, Mohammad Reza Aref, and Mehdi Rasti. 2022. Comprehensive Comparison of Security Measurement Models. *Journal of Applied Security Research* (2022), 1–69. https://doi.org/10.1080/19361610.2021.1981089

[6] Rafał Leszczyna. 2021. Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security* 108 (2021), 102376. https://doi.org/10.1016/j.cose.2021.102376

[7] Shari Lawrence Pfleeger and Robert K Cunningham. 2010. Why Measuring Security Is Hard. *IEEE Security & Privacy Magazine* 8, 4 (July 2010), 46–54. https://doi.org/10.1109/MSP.2010.60

[8] Anass Rabii, Saliha Assoul, Khadija Ouazzani Touhami, and Ounsa Roudies. 2020. Information and cyber security maturity models: a systematic literature review. *Information & Computer Security* 28, 4 (2020), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

[9] RIA (Estonian Information System Authority). [n. d.]. E-ITS. Portal of Estonian Information Security Standard. https://eits.ria.ee/

[10] Mari Seeba. 2022. Framework for Security Level Evaluation (F4SLE) E-ITS based ver 2021-1. https://doi.org/10.23673/re-372

[11] Mari Seeba, Sten Mäses, and Raimundas Matulevičius. 2022. Method for Evaluating Information Security Level in Organisations. In *Research Challenges in Information Science*. Springer International Publishing, 644–652. https://doi.org/10.1007/978-3-031-05760-1_39

[12] Edyta Karolina Szczepaniuk, Hubert Szczepaniuk, Tomasz Rokicki, and Bogdan Klepacki. 2020. Information security assessment in public administration. *Computers & Security* 90 (2020), 101709. https://doi.org/10.1016/j.cose.2019.101709

[13] Claes Wohlin, Per Runeson, Martin Höst, Magnus C Ohlsson, Björn Regnell, and Anders Wesslén. 2012. *Experimentation in software engineering*. Springer Science & Business Media. https://doi.org/10.1007/978-3-642-29044-2

Received 22 May 2023; accepted 13 June 2023