Ogunjimi, O.L.A., Afolorunso, A. A. & Olukomoro O. (2018).
Elicitation of SME Requirements for Cybersecurity Solutions
Through Adherence to Recommendations. *Advances in
Mathematical & Computational Sciences*
Vol. 6 No. 2, Pp 29-34

Article Type: Research Article
Manuscript Received: 13th May, 2018
Review Type: Blind
Final Acceptance:: 19th June, 2018
DOI: [dx.doi.org/10.22624/AIMS/MATHS/V6N2P4](https://doi.org/10.22624/AIMS/MATHS/V6N2P4)

³Department of Computer Technology, Yaba College of Technology, Lagos, Nigeria

Small and medium-sized enterprises (SME) have become the weak spot of our economy for cyber-attacks. These companies are large in number and often do not have the controls in place to prevent successful attacks, respectively are not prepared to systematically manage their cybersecurity capabilities. [Question/problem] One of the reasons for why many SME do not adopt cybersecurity is that developers of cybersecurity solutions understand little the SME context and the requirements for successful use of these solutions. We elicit requirements by studying how cybersecurity experts provide advice to SME. The experts' recommendations offer insights into what important capabilities of the solution are and how these capabilities ought to be used for mitigating cybersecurity threats. The adoption of a recommendation hints at a correct match of the solution, hence successful consideration of requirements. Abandoned recommendations point to a misalignment that can be used as a source to inquire missed requirements. Re-occurrence of adoption or abandonment decisions corroborate the presence of requirements. This poster describes the challenges of SME regarding cybersecurity and introduces our proposed approach to elicit requirements for cybersecurity solutions. The poster describes CYSEC, our tool used to capture cybersecurity advice and help to scale cybersecurity requirements elicitation to a large number of participating SME. We conclude by out- lining the planned research to develop and validate CYSEC1.

Keywords: Small medium-sized enterprises, cybersecurity, requirements elicitation

Small and medium-sized enterprises (SME) are considered as an important part of economy specially e-driven economies [1, 2]. Browne et al. explain that based on EU commission 2005, any company with fewer than 250 employees and with annual turn-over less than € 50 million can be considered as an SME [2]. Osborn with respect to EU Commission report states that these SME form 99% of European businesses [3].

Table 1. Cycle of requirements elicitation by studying adherence to recommendations.

Step	Elaboration	Example
1 Recommend theme	The cybersecurity expert offers a portfolio of topics that could be relevant for the SME.	Offering of ISFAM focus areas, covering organisational, technical, and support themes for cybersecurity.
Step	Elaboration	Example
2 Select cybersecurity theme	The person in charge of cybersecurity in the SME selects one of the cybersecurity topics suggested for improvement.	Choice of “secure software development.”
3 Recom-mend con-trols	The cybersecurity expert suggests a set of controls that offer protection against cyber attacks.	ISFAM-based suggestion of version control, source code and web scanning tools, defect management systems, and regression
4 Select controls to be adopted	The person in charge chooses among the controls and defines a date for review of the control implementation.	Choice of Git-based configuration and release management, Jenkins, and SonarQube with recommended security test cases.
5 Monitor adherence	The cybersecurity expert and person in charge check adherence to the selected controls.	The cybersecurity expert and the person in charge identify inconsistent use of Git in the development activities, indicating that some employees did not use Git as intended.
6 Obtain feedback	The cybersecurity expert elicits answers to ques- tions like “what value did the selected control deliv- er?” or “why did you not use the control?”	Involvement of the employees that were not using Git as intended showed that they did not understand the release management process and perceived the tool to be too complicated. These feedback led to the replacement of git with GitKraken, a graphical client for Git that was well

31

We are developing the adherence monitoring-based requirements elicitation method with two organizations that are experts in cybersecurity and four SME that are interested in improving their cybersecurity capabilities. These four SME have guided us through development process with useful information and through the discussions, we received interesting feedback regarding current frameworks. In about one year, we open the collaboration to further cybersecurity experts and SME with an open call for joining our work. The co-development approach allows us to understand the dialogue between the cybersecurity expert and the SME to the extent that it can be implemented in the CYSEC tool. The work with the experts allows us to understand important solutions and controls that are available and how they are used to address cybersecurity threats.

3. PLANNED RESEARCH

- RQ1. What are the hurdles and enablers of SME to adopt cybersecurity solutions?
- RQ2. Can the study of adherence to cybersecurity practice be used as a method of requirements elicitation for improving cybersecurity solutions?
- RQ3. Can requirements elicitation be automated by embedding the dialogue between the cybersecurity expert and the person in charge of the SME in the CYSEC tool?
- RQ4. What are the effects of the CYSEC tool-supported approach on cybersecurity capabilities of SME and solutions that support these SME?

The outcome of the research will be an improved understanding of the requirements of solutions that protect SME against cyber threats. We expect that CYSEC as a tool not only improve the SME's adherence, knowledge, and awareness but also help cybersecurity experts with requirements elicitation for solutions that help SME to become secure.

This work was made possible with funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 740787 (SMESEC) and the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The opinions expressed and arguments employed herein do not necessarily reflect the official views of these funding bodies.

REFERENCES

1. C. Valli, I. Martinus, M. Johnstone, "Small to Medium Enterprise Cyber Security Awareness: an initial survey of Western Australian Business", Proceedings of the International Conference on Security and Management (SAM): The Steering Committee of The World Congress in Computer Science Computer Engineering and Applied Computing (World-Comp), pp. 1, 2014.
2. Browne S, Lang M, Golden W. "Linking Threat Avoidance and Security Adoption: A Theoretical Model For SMEs", Bled eConference, p. 32-43, 2015.
3. E. Osborn. Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs. CDT in Cyber Security, CDT Technical Paper 01/15, 2014.
4. R. Lewis, P. Louvieris, P. Abbott, N. Clewley, K Jones, "Cybersecurity information sharing: a framework for sustainable information security management in uk sme supply chains", Proceedings of the European Conference on Information Systems (ECIS) 2014, June 9-11, 2014, ISBN 978-0-9915567-0-0.
5. Kuusisto, T., and Ilvonen, I. (2003). Information Security Culture in Small and medium size enterprises. *Frontiers of e-business research*, 431-439.
6. T. Kurpjuhn, "The SME security challenge", *Computer Fraud & Security*, vol. 2015, no. 3, pp. 5-7, 2015.
7. Zec, M., & Kajtazi, M. (2015). Examining how IT Professionals in SMEs Take Decisions About Implementing Cyber Security Strategy. In *ECIME2015-9th European Conference on IS Management and Evaluation: ECIME 2015* (p. 231).
8. S. Dojkovski, S. Lichtenstein, and M. Warren, "Enabling information security culture: influences and challenges for Australian SMEs," in *ACIS 2010: Proceedings of the 21st Australasian Conference on Information Systems*, ACIS, 2010, p. 61.
9. Z. Ng, A. Ahmad y, S. Maynard, "Information Security Management: Factors that Influence Security Investments in SMES", *Australian Information Security Management*, 2013.
10. T. Gundu, S. V. Flowerday, "Ignorance To Awareness: Towards An Information Security Awareness Process", vol. 104, pp. 69-79, June 2013.
11. Cholez, H. and F. Girard, Maturity assessment and process improvement for information security management in small and medium enterprises. *Journal of Software: Evolution and Process*, 2014, 26(5): p. 496-503.
12. F. Mijndhardt, T. Baars, M. Spruit (2016). "Organizational characteristics influencing SME information security maturity." *Journal of Computer Information Systems* 56, 2. 106-115.
13. R. J. Wieringa, *Design Science Methodology for Information Systems and Software Engineering*, Springer-Verlag, 2014.
14. <http://library.isical.ac.in:8080/jspui/bitstream/123456789/6553/1/Statistical%20method%20from%20the%20viewpoint%20of%20quality%20control.pdf>
15. K. Schwaber and M. Beedle, *Agile Software Development With Scrum*. Upper Saddle River, NJ: Prentice-Hall, 2002.
16. A. Fabijan, H. H. Olsson, J. Bosch, "Customer feedback and data collection techniques in software R&D: A literature review" in *Software Business*, Berlin, Germany:Springer- Verlag, vol. 210, pp. 139-153, 2015.