ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (23-25), Month: October - December 2021, Available at: www.researchpublish.com

Managing Cybersecurity Maturity Assessment within an Enterprise

[1]Ahmad Sirhani, [2]Abeer Shammari, [3]Mohammed Otaibi, [4]Eidan Aleidan

Saudi Aramco

Dhahran, Saudi Arabia

Abstract: **A Maturity Model is a widely used technique that is proven to be valuable to assess business processes or certain aspects of an enterprise. The evaluation of the Enterprise practices against the model — called an ‘‘assessment’’ — determines the level at which the organization currently stands. It indicates the organization’s maturity in the area concerned, enabling stakeholders to clearly identify strengths and improvement points, and accordingly prioritize what to do to reach higher maturity levels and see the greatest improvement and the highest return on investment. To make that possible, maturity assessments must be performed. A maturity assessment activity can range from simple self-assessment questionnaires to fully- fledged assessment methods. This (white paper/case study) sheds light on the use of multi-function organizations for managing fully-fledged assessments at an enterprise level.**

Keywords: **Managing Cybersecurity, Maturity Model, business processes.**

Figure 1

I. INTRODUCTION

Generally, IT organizations of any size focus on cybersecurity, business operations, and quality assurance to ensure business sustainability and service delivery.

Technology is advancing at a faster pace today than it ever has before and that is contributing to the fast-evolving risks to data security. This has demanded the safeguard of infrastructure, application and data, against any internal and external threat vectors aiming to exploit the unmitigated system vulnerabilities [1]. Apart from establishing robust security policies and practices, it is imperative to periodically scrutinize whether the controls are performing effectively as intended [2]. This scrutinization method is called “Cybersecurity Maturity Assessment” [2].

The cybersecurity maturity assessment focuses on specific controls and practices that protect critical assets, infrastructure, applications, and data by assessing the organization's defensive posture. The assessment also emphasizes operational best practices for each control area, as well as the organizational effectiveness and maturity of internal policies and procedures.

Although performing a full-fledged cybersecurity maturity assessment does take time and can temporarily interrupt some IT operations. The assessed organizations realize that there are benefits to the inconvenience such as:

- Gaining important insights into the organization's cybersecurity practices and how effective they are at preventing breaches [3] [4].
- Using the learned information to improve current cybersecurity measures or guiding organizations as to where new ones need to be added.
- Benchmarking the assessment results with similar organizations to help identify security trends [4].
- Preventing the organization from relying heavily on some security controls and ignoring others [5].
- Improving communication between employees, IT personnel, and upper-level management.

Therefore, to manage the assessment at an enterprise level with minimal interruption to the operation, the assessed organization requires having the right key individuals going through well-constructed processes with a technology that manages, tracks, and ensures the right implementation of those processes.

Assessed organizations can manage the cybersecurity maturity assessment flawlessly if they focus on the below three pillars [6].

II. THREE PILLARS

A. *Process*

"If you can't describe what you are doing as a process, you don't know what you're doing." – W. Edwards Deming.

Managing cybersecurity maturity assessment at an enterprise level requires a well-constructed process to move the immense number of tasks and activities throughout the stages of the assessment more efficiently. This could be achieved by having multiple processes or one main process supported by multiple sub-processes; and it started with forming a centralized team who act as a midway layer between the assessed organization and the external assessor [6]. This core team is responsible for executing the following processes:

- Conducting self-assessment to gain an immediate picture of where the organization need to improve and allocate resources
- Conducting collaboration sessions with subject matter experts (SMEs) to map practices with each of the function owners and accepting the ownership of the controls.
- Collecting and validating evidence with SMEs before being assessed by the external assessor, where actual practices and controls implemented on ground are verified for their robustness in meeting the organization's security requirements.
- Engaging with the external assessor in the enterprise assessment.
- Developing a gap closure plan with SMEs and Adapt Learning.

B. People

Executive management is the primary source of support during the assessment phases and can provide direction and assistance when necessary. Management involvement is a critical success factor, as it will ensure leaders are updated more frequently and recognize the gaps during the assessment [5] [6].

Another element of success to add for any assessed organization is the involvement of the right SMEs from IT operation. As SMEs will lead in addressing the requirement more efficiently during the assessment and gaps identification. The SMEs have the needed knowledge to analyze the information collected and add more clarification of the requirements during the maturity assessment.

Additionally, establishing a core team that manages the execution of the above-mentioned processes is crucial to the success of the assessment. The core team plays a major role in the assessment as they would be the focal point between SMEs, executive management and external assessors.

C. Technology

Having a proper solution to manage the maturity assessment has a crucial impact on handling the activities, such as logging, tracking, reporting and analysis. The solution can eliminate a significant amount of the introduced by the maturity assessment [6].

The solution is used by SMEs from different organizations to collaborate and participate in the assessment, ensuring that all tasks are completed in a timely manner. It allows having an efficient and easy mechanism to conduct the assessment by reducing the man-hours per activity and task.

From a flexibility and optimization perspective, technology enables organizations to boost engagement, identify gaps, and support the assessment objective by increasing the flexibility in handling the associated tasks, and improving the feedback mechanisms.

In addition, the solution provides analytical capabilities such as dashboards and tracking reports to ensure meeting the assessment expectation and deadlines. This would offer to management and SMEs, transparency and visibility throughout the assessment processes. Therefore, management will have deeper insight of each organizations' progress in terms of artifact submission, review and final acceptance.

Finally, the solution also enables quality assurance (QA) by allowing the core team to review and validate the submission of supporting documents and artifacts.

III. CONCLUSION

Many assessed organizations develop techniques to handle various maturity assessments; however, challenges that may arise could jeopardize the success of the assessment. Thus, the three key elements of process, people and technology must be well-structured and available in order to effectively handle the cybersecurity maturity assessments. The integration between the three elements leads to the desired results in a timely manner. Executive management, the core team and SME involvement is essential to secure organizational support during the execution. In addition, utilizing the proper technology by providing a user-friendly tool for managing the assessment and evidence, offers robust reporting and collaboration with SMEs. This will offer all involved stakeholders the ability to be consistently aware of the requirements and gaps.

REFERENCES

[1] N. T. Le and D. B. Hoang, "Can maturity models support cyber security?," in 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), 2016.

[2] R. M. Adler, "A dynamic capability maturity model for improving cyber security," in 2013 IEEE International Conference on Technologies for Homeland Security (HST), 2013.

[3] O. M. Al-Matari, I. M. Helal, S. A. Mazen and S. Elhennawy, "dopting security maturity model to the organizations' capability model," Egyptian Informatics Journal, vol. 22, no. 2, pp. 193-199, 2021.

[4] G. Drivas, A. Chatzopoulou, L. Maglaras, C. Lambrinoudakis, A. Cook and H. Janicke, "A nis directive compliant cybersecurity maturity assessment framework," in 020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), 2020.

[5] d. B. Rossouw and S. H. Von Solms, "Modelling Cyber Security Governance Maturity," in 2015 IEEE International Symposium on Technology and Society (ISTAS), 2015.

[6] D. R. Boccardo, L. M. S. Bento and F. H. Costa, "Towards a Practical Information Security Maturity Evaluation Method focused on People, Process and Technology," in 2021 IEEE International Workshop on Metrology for Industry 4.0 IoT (MetroInd4.0 IoT), 2021.