

Zachary Six

March 31, 2024

CYSE 200T

Professor Kirkpatrick

Determining the Best Suggested Course of Action for Cyber Security Department

In this brief report, I will be discussing a suggested course of action for an organization's cyber security department with a limited budget. I will provide the pros and cons of both in-house training and outsourcing of a cyber security department. After explaining these I will give my suggestion as to how to balance these ways of providing cyber security to an organization.

In-House Training

In-house training comes with many advantages including the ability to have employees who know the ins and outs of the system and can pass this information along to future employees. With employees having insight into the intricate details and quirks to the system, turn around for a patch or update for the system can arrive at a much quicker rate. The employees are also able to tailor new technologies to work specifically for certain vendors and integrate perfectly into existing systems (Villanueva, 2022).

Outsourcing the Security Program

While many organizations provide in-house security for their systems, many organizations rely on outsourcing their system security. Outsourcing security can provide a company with expert levels of cyber security knowledge and implementations, 24/7 support, and the simplification of compliance laws regarding information security (Glynn, 2023). Third-party

organizations that specialize in information security, meaning that the service you get will be quality and have experienced insight (Glynn, 2023). Because these organizations specialize in this field, many of them are able to provide 24/7 service to fight against cyber-attacks while in-house security teams may be small teams that also need to take periodic breaks.

Implementing In-House and Outsourced Information Security

Although having in-house cyber security has a multitude of advantages there are disadvantages including cost, performing the actual training, and purchasing cyber security technology to integrate into the organization. Outsourcing can have issues with system intricacies, sharing resources may cause delayed solutions, and the possibility of receiving very general solutions instead of needs tailored to your situation. Finding a solution that fits an organization's needs while keeping within a budget can be often difficult. By implementing a hybrid of the two options, an organization can address whether the problems should go to the outsourced company or be looked at by in-house IT staff. (Glynn, 2023)

Conclusion

Implementing a cyber security department can be quite costly to implement it in such a way that provides effective security, however, implementing a hybrid approach consisting of in-house and outsourced information security can provide the effective security while also being cost effective. To provide protection against organizational-specific programs and systems, employees should train oncoming employees on a "just-below-surface-level" basis that way they have more knowledge than the end user in case they need to provide baseline assistance. Outsourcing the IT staff can be effective in short-term periods when the IT staff hasn't quite

reached its potential and can also provide 24/7 support during a cyber-attack and implement specialized techniques. Overall, implementation of the hybrid approach can provide a cost-effective approach to the implementation of a new cyber security department.

References

- CrowdStrike. “How to Choose between Outsourced vs In-House Cybersecurity .” CrowdStrike, 2 Dec. 2022, www.crowdstrike.com/solutions/small-business/in-house-vs-outsourced-cybersecurity/.
- Glynn, Patrick. “What Are Pros and Cons of Outsourcing Cybersecurity?” Insight Global, 6 June 2023, insightglobal.com/blog/outsourcing-cybersecurity-pros-cons/.
- Villanueva, Mark Sheldon. “Outsourced or In-House Cybersecurity: What Are the Pros and Cons?” Intelligent Technical Solutions, 24 Sept. 2022, www.itsasap.com/blog/in-house-vs-outsourced-cybersecurity.