Isaac Flores

Professor Kirkpatrick

CYSE 200T

4 November 2024

Write Up: The Human Factor in Cybersecurity

Balancing the budget of a business is a complicated endeavor. Much careful consideration must be made regarding how much to spend on cybersecurity training and how much to spend on additional cybersecurity technology. Furthermore, it is important to consider the role of the person who decides this in organizations and businesses. The chief information security officer is usually the official of the company responsible for the information security department of an organization. This document analyzes the common needs a business has in association with cybersecurity training, technology, and budgeting.

Fujs et al. (2023), state, “This provides us with an opportunity to tailor information security-related software and training requirements to end user profiles thus increasing overall information security performance” (p. 1). To properly design a budget accurately reflecting the cybersecurity needs of a business, a CISO must tailor the budget to fit the needs of a business regarding both cybersecurity training needs and cyber technology needs. Another issue that a CISO might face is the aspect of a limited budget causing problems in meeting the information security needs of the businesses. This is especially prevalent in small businesses with small budgets for cybersecurity resources. This leads into the idea of investing in cost effective strategies. Fujs et al. (2023), state, “Additionally, implementing ineffective information security mechanisms needlessly raises the cost of the developed system” (p. 3). Technology spending

requires a considerable amount of consideration by the CISO as it can strengthen the cyber security effectiveness of businesses with a limited cybersecurity budget.

Recognizing the different aspects of what is needed for a cybersecurity budget to be used in a business can result in more efficient use of funds. One of these aspects of the technological side of the cybersecurity effectiveness within a company. Fujs et al., state (2023), “On one hand, different technical mechanisms, typically defined in iSSR, can be used to limit unsafe behavior” (p. 2). Software is an investment that takes continued spending as new updates for software are quite recurring. Software has the importance of providing tools and processes designed to safeguard digitized information of significant importance to a company. It can involve firewalls, intrusion detection systems, intrusion prevention systems, and network monetization services. Proper utilization of cybersecurity training is also an area of significant concern.

Cyber Security training is crucial in strengthening the human aspect of cybersecurity defense. Fujs et al. (2023), “On the other hand, training is typically used to improve knowledge, attitude and behavior of end users. We introduce iSTR to define such training” (p. 2). Training is used to improve social engineering mitigation techniques. Like software, training should be recurring as new cyber threats are a recurring issue due to advances in technology.Training should also be limited to focus on the individuals more in need of training compared to others. Fujs et al. (2023) state, “However, if only a few end users are below average in a certain information security focus area, it is probably better the option to train the poorly performing end users (iSTR)” (p. 4). As a CISO with a limited budget, specific downsides must be considered to improve the overall security of a business.

As the CISO of a business balancing a budget based on cybersecurity technology needs and cybersecurity training needs, I think that I would first start with considering the training

needs of the employees. I think the human aspect of cybersecurity should be considered first. Fujs et al. (2023) state, “The proposed approach builds on the idea that information security should be improved both by limiting the unsafe behavior of end users with technological solutions and by improving their information security related knowledge, attitude and behavior” (p. 2). Furthermore, humans may be a weaker link compared to software due to human error. I think the majority of the budget should be used in training the less knowledgeable and less skilled employees regarding cybersecurity best practices to avoid that cybersecurity vulnerability being exploited. Additionally, I would then consider the software requirements for the businesses. The importance of cost effective spending and meeting the needs of the businesses in regards to software security would be quite arduous. However, the remainder of the budget would fall entirely on the technology needs of the company. This plan is not perfect and has its flaws. However, this is my plan and view on how to best protect businesses with cybersecurity with a limited budget.

Both cybersecurity training needs and technology needs should be addressed by the chief information security officer within a business. Balancing the budget between these needs of a business can be an arduous task. Both training and technology are investments that can lead to recurring costs and needs as new advancements in training, best practices, and software may become available. I think it is important to place the majority of the budget on the greatest vulnerability within a business. This may result in more budgets being allocated to human cybersecurity training. However, the remainder of the budget would be left to the technology needs of the company.

Reference

Fujs, D., Vrhovec, S., & Vavpotič, D. (2023). Balancing software and training requirements for information security. *Computers & Security*, *134*, 103467. https://doi.org/10.1016/j.cose.2023.103467