Name: Eric Corpus

Date: April 9, 2023

Maximizing the Value of a Limited Budget – A CISO Dilema

A Chief Information Systems Officers primary responsibllity is to ensure the security of an organization's information assets. In a resource limited environment, it's important to balance between purchasing new technologies as well as investing in cybersecurity training. Both of these effect every organization at every level. While purchasing new technology can help an organization stay ahead of emerging threats, investing in training can keep your team informed about the most recent security trends and best practices (Kark and Agus).

A CISO should understand the importance of evaluating the organization's needs and goals before making any decisions. Understanding the costs associated with each option and how it will effect the budget is also a critical aspect to consider. While there are many possiblilities to consider prior to allocating money, a CISO may look to conduct a assessment of the buisness' current cybersecurity posture, weigh the pro's vs con's of how much technology vs training costs, identify whether the investments contribute to the overarching cybersecurity posture of the organization, or investments can be made based on the risk. These considerations will greatly inform how best to invest in either technology or training.

Assessing the cybersecurity posture of an organization can be conducted in many ways. The team that will completing this assessment to inform the CISO of the organizations security posture could look to NIST or ISO 27001 or look to a methodology to what best aligns with the organziations needs and requirements ("What Is a Cybersecurity Posture Assessment? | Hitachi

Systems Security"). The key take away to understand is that the assessment can help a CISO identify where investing in new technology would be most effective and where investing in training would be most valuable.

After conducting a cybersecurity assessment, there will likely be a range of recommendations for a CISO to consider. At this point, the CISO should carefully consider the costs assocated with the potential investments to determine the most effective approach. For example, investing in a new security tool may involve a significant upfront cost, but the could the potentially reduce the risk of a security breach and result in cost savings over time. On the other hand, investing in training may be a more affordable option initially, but ongoing investment may be necessary to ensure that the staff are kept up-to-date with the latest security threats and best practices.

The next step to consider is to understand the impact each investment would have on the organizations overall posture. There could be results that identifiy that a significant number of incidents were caused to to operator errors. That could be interpetted as a greater need to invest in training. Another consideration would be looking at whether a SIEM system would be worth the investment. These SIEM systems enhance cybersecurity posture by providing greater visibility to threats allowing security teams to respond more quickly and effectively.

As a CISO, determining the impact of investments in technology or training requires a holistic approach taking into account a wide-range of factors. Since CISO spend the majority of their days managing risk, it would make sense that when considering where to invest money is to possible prioritize spending based on the risk's the organization faces alone. If there are ciritcal assests that are of high risk of compromise, then spending in that direction makes sense.

However, if the risks are low at having a security incident, you may prioritize investing in training instead. Sometimes there is a event that is unforeseen that affects the ability for a CISO to take their time in evaluations. The COVID-19 pandemic, for instance, accelerated the adoption of technology across many businesses, which embraced new digital tools to survive. While many organizations set up websites or e-commerce platforms to process online orders, a sizable portion were less willing to take the chance (Dineva).

When a CISO looks to prioritize allocation of funding, whether it be towards investments in technology or spending to better training the workforce, there are many issues to consider. A consideration that may be overlooked is to read and evaluate what a CISO's peers are doing to enhance their organizations cybersecurity posture or are there ways to that they are being trained better. A potentially glaring issue with investing in technology is that fact that there may be results of a decrease to the workforce. The continual improvements of AI technology for example potentially takes jobs away from call center type customer service. I could potentially see CISO considering limiting training opportunities for employees because there are some that believe that that only results in training someone to leave and take a better job with the training they received from their old job. At the end of the day, I would look to prioritize based on risk with the overall goal of ensuring the organization can continue to do what makes profits and keeps the organization from going under. Its with this level of responsibility that CISO's role is gaining more importance each and every day.

References

Dineva, Sonya. “Convincing Your Company Leaders to Invest in New Technology.” *Harvard Business Review*, 18 Jan. 2022, hbr.org/2022/01/convincing-your-company-leaders-to-invest-in-new-technology.

Kark, Khalid, and Taryn Aguas. “The New CISO: Leading the Strategic Security Organization.” *Deloitte Insights*, 26 Jul. 2016, www2.deloitte.com/us/en/insights/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html.

“What Is a Cybersecurity Posture Assessment? | Hitachi Systems Security.” *Systèmes De Sécurité Hitachi*, hitachi-systems-security.com/what-is-a-cybersecurity-posture-assessment. Accessed 7 Apr. 2023.