Myrna E. Santiago

11/12/2023

CYSE 200T_17570

BALANCING CYBERSECURITY: CISO APPROACH

A CISO (Chief Information Security Officer) is a high-ranking officer of a company. They are in charge of the security over the information, network and technology of the organization. They need knowledge not only in the technology area but also in finances, social science and the different approaches in cybersecurity. This paper will show some of the different hats that the CISO has to wear, their daily struggles with economics and security, and solutions for those problems within a budget.

CISO Responsibilities

Some of the CISO responsibilities are:

- The development and implementation of processes and systems, from prevention to recovery from cyberattacks.
- The implementation of GRC (governance, risk and compliances) of the cyber process.
- The development and implementation of training and education of users.

These are some of their responsibilities. Many CISO's do a lot more and their new roles are constantly changing, to the point that companies are recognizing them as co-equals with the Chief Information Officer of the organization. (Cisco, n.d.)

The Problems

A CISO has multiple problems to address everyday but we can identify three major ones, economics, end-user education and control of resources. Even in the current environment with attacks happening every few seconds many companies refuse to invest heavily in data security. Add to that a possible economic recession that has been looming over us for quite some time and many companies continue putting at risk their data and resources to accomplish some revenue and keep share holders happy. The problem with this view is that cyber attacks have become a problem of epic proportion to every organization around the world. The ifs have been taken out of the equation and it is mostly to when it is going to happened. If an organization has any kind of technology, the risk for an attack is there, period.

Another problem is end-user education. Many companies put together a comprehensive security training, but do not enforce it. Many times, they just tell a person to read it and sign at the bottom of a page. Enforcement is more that read here and sign there but make a person practice what they read. Without practice many skills are lost. If the person does not use what they learn into their normal lives it is like they never learn it at all.

Last, but certainly not least is that many companies make each department apply their own security following the guidelines in place. The biggest problem is that a CISO will be dependent on how each department head will spend in security and deploy said tools. It will also present a problem as to how the users in each department is train. Having to many tools is as bad as not having any if the results differ greatly from each one, creating new problems for the CISO and the organization overall.

The Solution

A good security program has three important characteristics, transparency, accuracy and precision. Transparency can be achieved by using a framework like NIST or ISO. Frameworks are very abstract, but it provides room for interpretation that can help guide the organization on the right path. That is when accuracy and precision come into play. By identifying the possible threats, a specific organization can have an accurate map can be create of how to defend from those threats. The precision comes in the form of which tools to use any given time to save money and time. (Isles, 2023)

The Implementation

With the help of an accurate map we can then evaluate six action areas:

1. First, we need to identify the risk vs spending. Which areas required a more rigorous control and which ones can take the hit an survive. If the investment is bigger than the losses then that money can be use for protection in other more impactful areas. (Savings between 5 and 10 percent)
2. Second, evaluation of projects helps save money by resolving conflicts and overlaps and deciding of balance vs cost. A simple project may not need the same amount of money that one that requires high security because an innovating tool or product is going into development. (Savings between 5 and 10 percent)
3. A review of security operations, can help identify operational efficiency. Can we renegotiate service level agreements? Can we automatize a tool or

train an existing employee and raise his/her pay instead or bringing someone in and have to train and pay an additional salary? Are the resources fully aligned with the requirements? By asking these questions a company can save between 5 and 10 percent of the budget.

4. Rationalize tools. By checking all existing tools and verifying their use we can identify those that are not needed or outdated. Do the tools are being use to the full potential? Are new tools out there that are similar in cost but have the tools we need in a single package? Is the tool complicated that we need to hire someone new or can we train our current employees in them and save money? These rationalizations can save between 5 and 10 percent of a budget.
5. Review all the data acquired in the previous step. By analyzing if its cheaper at a long run bring in 5 new employees with knowledge in the necessary tools instead of outsourcing the need to third party vendors the company can save a lot of money and possible breaches in the future. Outsourcing can be a good thing if the company is an international one with multiple locations or a medium one with limited space or capabilities in terms of technology. But outsourcing also bring an increase risk of threats because the third party needs internal access that can be detrimental in the long run.
6. Improve the model. Check for overlapping roles, tools that duplicate processes, and how much control each department have in which areas. Do they need that much control? How risky it is for the company as a

whole? Do the employees need access to those resources or it is not necessary? (Bartol et al, 2023)

Conclusion

By creating the right road map, we can save money and get a more control environment. As a CISO, I will follow the prior steps, and create a comprehensive proposal to present to the executives in charge. Once a consensus is achieved, I will create a balance between education and tools needed. The education will be an interactive and creative one, that way it will become a constant practice inside the organization. Maybe with some incentive every quarter for each department to achieve, people are motivated when positive reinforcement is added. In terms of control, I will add some control measures that rely information directly to one team that can react proactively. This will keep each department having certain amount of control. Each department head will need to communicated why they need to spend money in a certain tool or software related to cybersecurity and how it can affect the overall performance of current network. This plan will help save money and secure the organization.

Reference

Cisco. (n.d.). *What is a CISO?* Cisco. https://www.cisco.com/c/en/us/products/security/what-is-ciso.html.

Isles, A. (2023, May 23). *Where to Focus Your Company's Limited Cybersecurity Budget?* Harvard Business Review. https://hbr.org/2023/05/where-to-focus-your-companys-limited-cybersecurity-budget.

Bartol, N., Weingberg, C., Pasupathinathan, V., White, C., & Moore, N. (2023, August 28). *Reducing Cyber Risk on a Tight Budget.* BCG. https://www.bcg.com/publications/2023/how-cisos-are-reducing-cyber-risk-on-a-tight-budget.