

Charles W. Pridgen

April 6, 2024

The Human Factor in Cybersecurity

In this writing I will take on the role of a Chief Information Security Officer (CISO). Being CISO, I will describe how I would allocate the limited funds I have for training and additional cybersecurity technology, as well as the reasoning behind my decisions.

Allocation of Funds

A large bulk of my funding, equal to or less than $\frac{3}{4}$'s, would go to the cyber technology needed to properly secure our information systems and data. As far as the remaining $\frac{1}{4}$ of funds, they will be poured into training programs and applications used to educate and prepare the employees on cybersecurity and the different threats.

Why $\frac{3}{4}$ to Cyber Technology?

Confidentiality, integrity, and availability (CIA) are the three foundational elements of cybersecurity. Not only do these three elements create a more secure and efficient business, but it also creates excellent customer service, providing the feeling of security and confidence knowing their personal information is in safe hands. Without cyber technology employees will be able to access any data they want, and sensitive information will be exposed. Data/information could be altered or deleted, compromising its integrity. In the event of a catastrophe, without any back-up plans or alternate databases, critical business data will be lost, and operations will not be able to resume in a timely manner costing the company money, and possibly putting it out of business. Effective and reliable technology will allow the business to operate more confidently and efficiently. Cybersecurity technology is expensive, especially for reliable/effective equipment, and without it there is no CIA. A plethora of problems will arise, so to combat these threats, I

will bolster our cybersecurity technology reliability and capability. For those reasons, I believe ¾'s of the budget should go to cyber technology.

Why ¼ to Training?

Outside of the technology, people pose the greatest threat and are a major reason for the need of cybersecurity, whether it's trusted employees or strangers from across the world. Social engineering attempts like phishing, pre-texting, deep fakes, etc. constantly pose a threat to companies, and attackers are getting a lot more effective with their attempts. Phishing emails and texts are looking more and more legitimate as time goes by. Without any training, employees will surely fall for these attacks and other social engineering threats. Educating the employees of the different threats, red flags associated with them, and how to respond to them are crucial for the success of the company. Employees in the company, one way or another, will have access to the network, databases, files, etc., which puts them in the crucial role for providing quality cybersecurity. Human threats are not only cyber, but physical to. There are obvious physical threats like someone trespassing and trying to gain access to an employee computer who shouldn't be. Some physical threats might not be as obvious, like an insider threat, or ignorantly plugging in a USB found on the ground to a computer connected to a secure private network. Even with all the cybersecurity technology in the world, if Jane Doe decides it's a good idea to allow the mysterious masked man to use her computer to check out what he has on his USB, my cybersecurity efforts will be futile. Without proper training, employees essentially become unintentional insider threats, and since completely ridding the human factor is not possible, as first line defenders, we need consistent, quality training to create more reliable, secure cybersecurity.

Conclusion

Data confidentiality, integrity and availability are the three main elements of cybersecurity. Employees do play a crucial role in cybersecurity, which is why I believe no less than $\frac{1}{4}$ of the budget needs to go to training these first line defenders. Without it they essentially become unintentional insider threats themselves, however, without cyber technology, there is nothing to protect, and even with training, cybersecurity events are still going to occur. Cyber technology is very expensive, but without it there is no CIA. Due to these reasons, $\frac{3}{4}$'s of the budget will be allocated to cyber technology for more quality/reliable equipment that will help bolster the company's data confidentiality, integrity, availability, customer service, and cybersecurity posture.