If I were CISO, I would split the budget 40/60 between training and technology. Nearly equal weight given to both will help to ensure that the company is protected from both the cyber side and the human side. Good cyber tools and technology can stop deliberate threats and attacks on an organization, but there's always a possibility that an attack can come through because of employee negligence.

Training is important because it provides the awareness of threats to the non-cyber employees. The people who don't work in cybersecurity will be able to recognize issues like phishing attempts or insider threats. Oftentimes, a company becomes vulnerable to attacks because of human error or ignorance. By eliminating the vulnerabilities at the employee level, the company reduces the liability of the average employee. Cyber tools can be effective if there is a team that knows how to utilize them, but they can't do much to stop an employee clicking on a phishing link and giving their password. Repeated, periodic training would reinforce the knowledge and awareness and make it more likely that employees will be alert for threats. Training that also includes instruction on what to do when a threat or a vulnerability is detected helps to mitigate damage done. If employees are exposed to situations where a threat has been detected, they can practice what to do in those situations. Employees wouldn't be caught off guard and would be able to alert the cybersecurity team of any issues.

Cybersecurity tools still play a major role in detection and the prevention of attacks. As CISO, I would want to dedicate resources to provide extensive logging, scanning, and threat intel among other things. Having dedicated teams for cybersecurity and the tools does a lot to mitigate the potential for attacks. It's important to have knowledgeable experts to be able to use the tools and guide the company through best practices in cybersecurity. A cybersecurity team, or even an IT team, can direct resources to where they are needed and can interpret data with cybersecurity in mind. Tools can also take care of a lot of the legwork needed to analyze data and provide a wide net of protection. While it is possible to dedicate a whole budget towards technology to take care of the majority of areas of concern, they cannot prevent everything. A good cybersecurity team should have the tools to prevent attacks and take care of systems, but should not solely rely on them to protect the whole company.

In conclusion, it is much easier to prevent attacks than to clean up after them. In my opinion, cybersecurity requires active participation from both the cybersecurity teams and the employees themselves. Dividing the budget for 40% training and 60% technology would help both the cyber teams and the employees do their part to protect the company.