India Henry

CYSE200 - 9:30 am

31 March 2024

The Human Factor in Cybersecurity

This paper will debate the pros and cons of spending more money on educating already existing employees or hiring cybersecurity experts. The preferred method would be to educate already existing employees but also understand that in order to educate those employees efficiently, hiring experts may be necessary.

Educating Employees

Allocating money to educating employees has a multitude of pros. Firstly, educating your already existing employees makes them more valuable to the company. It doesn't really matter if new personnel are hired if the already existing employees still don't take proper precautions. By allocating money to already existing employees to learn how to safeguard their accounts it increases the security of the company without having to hire an entire new team to manage the security of the company.

This would also build employee relations with the company. Being educated in cybersecurity makes employees more marketable and valuable to companies, so even if they don't stay at the company that is providing them the learning experience, they would still be appreciative of getting to learn. This can also build employee loyalty to the company that is teaching them cybersecurity skills because it shows the company is willing to invest in its employees instead of demanding skills they don't know, hiring new personnel to take care of the issue, or even hiring replacements for the employees that already know the skills to "save money"

Hiring Experts

Hiring cybersecurity experts could also be a good route to take because companies do need to have experts to help guide their company to be more secure. Hiring new personnel can be beneficial to developing companies because all companies need cybersecurity and it may be a better investment to hire someone who already knows the basic protocols than to hire someone who has to be taught them. This is a bit more complicated for the already developed, bigger, companies that have multiple teams of personnel that aren't educated in cybersecurity. Those companies may also see value in hiring experts, but maybe not hiring entirely new teams of cybersecurity experts as either an addition to the company or to replace already existing employees.

New Technology

It is always important to keep technology upgraded. New technology has a tendency to have security upgrades that old technology lacks, so investing in new technology is integral to the security of a company. There should be money set aside for upgrading technology when needed because not only is new technology generally more convenient, but it also usually has security updates that may not be offered on older devices.

Proposition

The best way to go about allocating money for a big company is to focus on educating already existing employees. That doesn't mean that hiring experts isn't a good idea. Bigger companies usually split their employees up into teams, one way to go about educating existing employees is to hire one expert per team to ensure any process that gets carried out is secure. Another way that would be investing entirely in existing employees is requiring and providing certifications that would need to be assessed annually. More money should be invested into employees than new technology, but a portion of the budget should always be allocated to keeping the technology as up-to-date as possible until new technology is needed.

Conclusion

Promoting cybersecurity in businesses can be costly but is worth the money spent on it. With a limited amount of money to allocate to support cybersecurity, it is a better idea to allocate more money to educating existing employees than to hire new personnel. New technology will be needed in order to keep companies secure, new technology should not be the company's top priority. It doesn't matter if the technology is new if the employees don't know how to work it.