Name: Trey Kirk

Date: 11-18-2022

Budgeting a Cyber Security Business

Through research about the different aspects of a cybersecurity department, multiple articles describe the changes cybersecurity has faced and evolved into since the covid-19 pandemic. Additionally, the articles described what it takes to get trained to become a cybersecurity specialist and how critical it is to have a department for cyber security within a business.

Funding Cybersecurity

In the world of business, information is one of the keys to success for a company. Large-scale companies know this and work to protect their confidential information. However, with the rise in cyber threats, it has become more costly to suffer from a cyber attack than to allocate resources to a cyber security department. In 2021 alone, data breaches have amounted to an average of almost $5 million in costs for an organization (Cyber Security Market Size & Share Report, 2030, n.d.). If a business were to allocate $500,000 to their cyber security department, they should allocate 45% of funds toward technical resources, 30% of funds toward training employees, and 25% of funds toward any additional technology.

Technical Resources

Businesses should allocate 45% of their cybersecurity budget toward technical resources. Technical resources include any of the major resources a cybersecurity department would use such as massive company servers, computer systems, and setting up VPN networks. Before the

start of the covid-19 pandemic, business may have allocated more funding toward technical resources, however, with the change of people working from home it can be shortened. Before the pandemic, 29% of the U.S. workforce worked remotely until 2020, which increased to 50% (Cyber Security Market Size & Share Report, 2030, n.d.). However, with the rise of the remote workforce, it opens companies up to more risks as people use their personal devices and home networks. Even with this heavy risk, it opens the company to allocating more resources to other sections of the department and spending any funds needed on fortifying the employees' at home network.

Training and Additional Technology

Companies should also allocate 30% of funds toward training their employees. Cyber security certifications often range from a few hundred to a few thousand dollar and can take from a couple days to a couple years to complete (How Much Do Cybersecurity Certification Programs Cost?, n.d.). If companies were to fund this certification training, it could help to reduce the shortage in cybersecurity specialist which could overall reduce the number of cyber-attacks around the world. Additionally, if companies were to offer this certification funding, it could bring more people to their company in support of cyber security. Companies should then allocate 25% of funding toward any additional technological resources. As new technologies arise, new forms for cyber threats emerge. This means cybersecurity specialist need to be accustomed to any new forms of technology that comes out to better protect assets.

Conclusion

Overall, cybersecurity is becoming a critical department for businesses that they must allocate resources to if they want to succeed. In whatever budget a business gives toward the

department, they should invest 45% toward technical resources, 30% toward training employees, and 25% toward any additional resources. The world of cybersecurity is expanding fast so the priority in the allocation of resources is also changing with time.

References

Cyber Security Market Size & Share Report, 2030. (n.d.). Retrieved November 18, 2022, from Grand View Research: https://www.grandviewresearch.com/industry-analysis/cyber-security-market

How Much Do Cybersecurity Certification Programs Cost? (n.d.). Retrieved November 18, 2022, from Noodle: https://www.noodle.com/articles/how-much-do-cybersecurity-certification-programs-cost