Mitigating the human risk factor

With the average cost of a data breach being well over 120,000 dollars for small businesses it is important that the budget for cybersecurity is used in the most effective way possible between cybersecurity technology and employee training to decrease the chance of a cyber-attack being launched on the business. With a multitude of free training available online, I believe it is best to focus more on the technology aspect of mitigating risk. (For this example, the business is moderately sized, with 500 employees and a 10,000-dollar budget).

Technology

Most of the budget will go towards advancing the cybersecurity technology available for the business. The company plans to begin by purchasing Mcafee ultimate protection for all employees. This technology, in large parts, can help protect employees from their own mistakes. The software features an antivirus, a VPN with 256-bit encryption, Web advisor web protection to warn employees of risk websites, PC optimization to boost overall performance. (McAfee+ ultimate, n.d.). The software also features Quickclean, which removes short-term files and cookies to keep exposure low, and a Shredder to securely delete files. Mcafee also features a password manager that is also capable of creating complex passwords for employees that struggle to do so. Mcafee’s vulnerability scanner can alert employees to possible security weaknesses in their devices such as needed updates. The identity monitoring service will also help employees to keep their records safe on the internet and comes with dark web monitoring for email. Mcafee also has a virus protection plan that would provide the company with reimbursement if a virus were to infect an employee’s device and was unable to be removed.

(McAfee+ ultimate, n.d.). Many of these features will help with warning employees against social engineering attacks that could put the company at risk. It would cost 2 thousand dollars to install Mcafee Ultimate on all employee devices, an additional 500 dollars would also be planned to be saved for possible future employees. The software can also be transferred from one computer to another if an employee must change devices due to another one breaking.

In addition to Mcafee the company also plans to spend 3 thousand dollars on SolarWinds Security Event Manager. The primary function of this service for the company would be to help defend against denial of service(DoS), attacks. The service can find and monitor network events and can obtain attacker IPs as well as block them. (Security event manager, n.d.).

The final technological investment for the company is Duo two factor authentication. It would cost 1,500 to purchase Duo for all employees, however it would allow employees to authorize their log in credentials through their cellular device, as a final add on to boost company security.

Training

With most of the cybersecurity funds going towards technology, employee cybersecurity training will be through an EdApp free course. The course introduces employees to several different types of cyber-attacks they may be vulnerable to and teaches them how to detect and identify them. Employees will also learn how to handle suspicious emails and websites. The second course further teaches employees about common internet scams and how they can identify and report those scams. The courses are online and can be completed on a cellular device or computer, the course tracker also allows for each employee’s progress to be tracked. (Top 10 free cybersecurity training for employees, n.d.).

Instead of spending the remaining budget on training, the company could use the remaining budget to offer employees incentive for completing their training.

The remaining 3,000 dollars could be split into 6, 500-dollar bonuses that can be distributed to employees that either show the most cyber awareness or do the best in the course. Not only will a possible yearly bonus increase the possibility of employees taking their cybersecurity training seriously, but it will boost morale overall and lead to the company getting better as a whole.

Conclusion

With small businesses being the biggest target for cyber-attacks, it is important the company uses every dollar of its cybersecurity budget efficiently. Overall, by allocating most of the funds to cybersecurity software, taking advantage of free training offered online, and offering monetary incentives for cyber efficient employees, the company can maximize the level of defense set up for employees, while also increasing employee morale and cyber awareness.

References

How much should your SMB budget for cybersecurity? business.com. (n.d.). Retrieved November 20, 2022, from https://www.business.com/articles/smb-budget-for-cybersecurity/

Keary, T. (2022, September 28). *8 best ddos protection tools & anti-ddos software 2022 (Paid & Free)*. Comparitech. Retrieved November 20, 2022, from https://www.comparitech.com/net-admin/best-ddos-protection-service/

McAfee+ ultimate - our most comprehensive online protection. McAfee. (n.d.). Retrieved November 20, 2022, from https://www.mcafee.com/en-us/products/mcafee-plus-ultimate.html

Pricing. Duo Security. (n.d.). Retrieved November 20, 2022, from https://duo.com/editions-and-pricing

SolarWinds. (n.d.). *Security event manager - view event logs remotely*. SolarWinds. Retrieved November 20, 2022, from https://www.solarwinds.com/security-event-manager?a_bid=d12100dc&CMP=BIZ-PAP-CMPRTCH-SecurityEvntMngmt-SEM-LM&data1=221019&data2=&a_aid=BIZ-PAP-CMPRTCH

Top 10 free cybersecurity training for employees. EdApp Microlearning Programs. (n.d.). Retrieved November 20, 2022, from https://www.edapp.com/top-10-cyber-security-training-for-employees