What are the costs and benefits of developing cybersecurity programs in businesses?

Amy Lawson-Gunkel

26 September 2019

Details

Businesses of all sizes should be investing their resources into developing cybersecurity programs into their operations; it is an even greater benefit for small businesses to take extra measures to protect themselves, since they have more at stake.

To begin developing an effective means of defense, the business should identify their vulnerabilities; by doing so, the organization may be able to identify risks they had not even known were present. These risks can exist within their employees. To best avoid an internal attack, the business can conduct background checks, create individual accounts for each user, or use the least privilege rule; the least privilege rule limits each user to appropriate minimum levels of access while still allowing them to effectively perform their job. Once risks are identified, it is time to instill protective measures; efforts should be directed toward: firewalls, filters, physical/logical security, and software updates. The purpose of the protective function is to "[support] the ability to limit or contain the impact of a potential information or cybersecurity event" (Small Business Information Security: The Fundamentals). Maintaining a satisfactory level of protection will assist the business with timely detection of any events; should an event occur, the way the organization responds will determine how significant/insignificant the outcome will be. The final, and most important, step in developing a cybersecurity program would be the recovery step. If the business is consistent about backing up their information, and in some cases purchasing insurance, they can continue their normal operations with minimal impact.

Although creating and maintaining a cybersecurity program can be demanding both on the company's employee and their budget, the investment of protection hold a high return. If the business can ensure the safeguarding of their customers' sensitive

information, then they should be able to maintain and expand their data base of clients; this in turn will help them expand the company to fit their business model.

References

06a - CyberSec for Small Businesses.pdf. (0AD). Retrieved September 26, 2019, from https://drive.google.com/file/d/1Jiu7kIrdkqTYAqu6Le2NaDr6JodJ5g2Y/view.

Paulsen, C., & Toth, P. (2016, November). Small Business Information Security: The Fundamentals. Retrieved September 26, 2019, from https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.