Budgeting for Cybersecurity

[Author’s name]

[Institute’s name]

Budgeting for Cybersecurity

**Summary**

The central objective of corporate governance is linked with the selection and application of appropriate approach of budgeting for cybersecurity. The broad idea of budgeting associated with active consideration of proper planning and planning by selecting the most accurate strategy to reduce the risk of costs. This form of consideration of critically vital when it comes to identifying different forms of risks responding to cyberattacks appears for Red Clay Renovations Corporation. A timely exploration of various forms of risks requires a suitable application of investment to meet the standards of protective cybersecurity effectively and efficiently.

**Identification of Risks**

           Identification of potential risks is the first and crucial step to ensure the successful allocation of financial resources in case of a company’s cybersecurity. The perspective of financial resources can determine by the domains of people's investment, process investment, and technology investment. It is important for the management to invest in these specific practice areas according to the requirements of the IT security program (Bowen, Hash, & Wilson, 2007). Identification of potential risks is the first practical step to select an appropriate strategy according to an organization’s requirements. The potential risks for the company recognized as follows:

· Improper protection of the business record

· Insignificant collaboration between different departments to meet the objectives of system policy.

· The risk of data theft in case of client’s personal information

· Incorrect forms of collection, analysis, and preservation of important information

· Improper application of offering renovation services.

**Selection of Strategy**

A decrease of possible cost in case of cyberattacks requires the selection of the most appropriate strategy according to the organization’s needs. It is important for the decision-makers to consider a specific strategy by correctly follows associated guidelines and plans of action. Minimize exposure is a strategy selected for Red Clay Renovations to reduce the potential cost of the problem of cyberattacks. The central aim of this practical strategic approach is to minimize the connection of information systems with other aligned and hazardous aspects.

           The basic idea of minimizing exposure as the strategy is that information systems are susceptible when it comes to the approach of accessing by others. The risk factors are immensely high that establish that important organizational information can be accessed or corrupted referring to the existence of data in the system. The strategy of minimizing exposure can be further characterized into two main elements. The first practical approach is that minimizes the existing linkages between a system and many different outside factors. The other idea of consideration is to reduce the levels of information and relevant procedures (Davis et al., 2016). This phenomenon can be mainly observed in the case of the active installation of software programs and the facets of information access through the system. Moreover, critical evaluation of internal links of the system is also a vital practical measure to restrict the entire damage from external attacks.

**Application of Strategy in Planning and Programming Phases**

           Alignment of minimizing exposure as a suitable strategy for the stages of planning and programming is the necessary condition to successfully achieve anticipated objectives of cybersecurity. Appropriate classification of different organizational resources in the forms of various classes or groups is a necessary condition to obtain the requirements of the planning process. Dissemination of physical and virtual resources is helpful for the organization to minimize the chances of data access categorized in the form of access. The objective of programming can be attained by implementing different interrelated organizational factors. The practical idea of programming requires reducing the networked instruments to minimize the chances of potential risks. Additionally, it is also critical to limit network access paradigms according to the organization’s requirements (Chew et al., 2008). The risks of unwarranted access to sensitive data need to be regularly scrutinized by determining a proper amount of physical and financial resources.

**References**

Bowen, P., Hash, J., & Wilson, M. (2007). Information security handbook: A guide for managers. *NIST SPECIAL PUBLICATION 800-100, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*. Citeseer.

Chew, E., Swanson, M. M., Stine, K. M., Bartol, N., Brown, A., & Robinson, W. (2008). *Performance measurement guide for information security*.

Davis, J. I., Libicki, M. C., Johnson, S. E., Kumar, J., Watson, M., & Karode, A. (2016). *A framework for programming and budgeting for cybersecurity*. RAND Corporation Santa Monica United States.