European Scholar Journal (ESJ)
Available Online at: https://www.scholarzest.com
Vol. 1 No. 4, December 2020,
ISSN: 2660-5562

DATA SECURITY FOR BUDGETING AND FORECASTING PROCESS

Kevin Maxon,
University of Plymouth, United Kingdom
Amit Deshpande,
University of Plymouth, United Kingdom
December 2020

Article history:

Received November 28th 2020
Accepted: December 7th 2020
Published: December 30th 2020

Abstract:

Data privacy refers to the appropriate use of data supplied to organizations for agreed-upon purposes. Customers' data should be adequate to meet their business requirements and wants; it should be accepted and supplied to them with full disclosure information. For failing to provide proper data privacy disclosure to clients, the Australian Federal Government continues to enforce penalties. Personal Identifiable Information (PII) is a term used to describe data collected in the banking and financial services industry. The confidentiality (protecting private information from unauthorized individuals), availability (providing timely access to information to authorized users), and integrity (protecting the accuracy, reliability, and validity of data and databases) of information are the primary concerns of information security. Computer security also includes issues such as authentication (ensuring that people using the system are who they say they are) and nonrepudiation (ensuring that a legitimate user cannot deny using the system). Firms must also be able to detect and fix data security breaches after they occur. As a result, information security refers to a set of actions aimed at safeguarding data and information systems.

Keywords: Financial analysis, Budgeting, forecasting, data security, cyber security, prediction

INTRODUCTION

The confidentiality (protecting private information from unauthorised individuals), availability (providing timely access to information to authorised users), and integrity (protecting the accuracy, reliability, and validity of data and databases) of information are the primary concerns of information security. Computer security also includes issues such as authentication (ensuring that people using the system are who they say they are) and nonrepudiation (ensuring that a legitimate user cannot deny using the system). Firms must also be able to detect and fix data security breaches after they occur. As a result, information security refers to a set of actions aimed at safeguarding data and information systems. Data security is defined by the confidentiality, availability, and integrity of data. Data security refers to the fact that it can only be accessed, used, and processed by those who have been given permission to do so. Data security ensures that data is available, reliable, and accurate. A data security plan ensures that only necessary data is acquired, that it is kept secure, and that any data that is no longer required is discarded. Security refers to a system's ability to protect itself from external attacks (Deliberate or accidental).

Secured systems are dependable and ready when they are needed, which makes them trustworthy. Secured systems that perform as planned without failures or delays assist the banking and financial services business achieve its goals. Cloud technology is a new upgrade for a more efficient processing system that uses the cloud as a warehouse to store data and make it easier to access when needed. This should be used in addition to manual data storing in our storage devices. Budgeting for information security expenditures is a critical resource allocation choice, regardless of whether they are classified as capital or operational costs. From an economic standpoint, businesses should invest until the last dollar invested in information security generates a dollar in savings. To put it another way, information security investments should be weighed in terms of cost-benefit analysis. The cost-benefit analysis utilizing the net present value (NPV) model is a well-established rational economic technique for budgeting capital investments.

DATA SECURITY

Data security is defined by the confidentiality, availability, and integrity of data. Data security refers to the fact that it can only be accessed, used, and processed by those who have been given permission to do so. Data security ensures that data is available, reliable, and accurate. A data security plan ensures that only necessary data is acquired, that it is kept secure, and that any data that is no longer required is discarded. Security refers to a system's ability to protect itself from external attacks (Deliberate or accidental). Secured systems are dependable and ready when they are needed, which makes them trustworthy. Secured systems that perform as planned without failures or delays assist the banking and financial services business achieve its goals.

PROTECTION OF DATA

Data privacy refers to the appropriate use of data supplied to organisations for agreed-upon purposes. Customers' data should be adequate to meet their business requirements and wants; it should be accepted and supplied to them with full disclosure information. For failing to provide proper data privacy disclosure to clients, the Australian Federal Government continues to enforce penalties. Personal Identifiable Information (PII) is a term used to describe data collected in the banking and financial services industry. It's used to make sure the customer is who they say they are.

Once data has been kept in the cloud, cloud service providers must decide on data security, which is one of the most important factors to consider. To avoid unauthorised access to customer data by third parties, cloud service providers must ensure data integrity, privacy, access denial, and the ease of confirming security. All businesses, profit or not, have begun to use the cloud for data storage, resulting in a security and privacy risk for data stored in the cloud. Furthermore, data transmission and cloud service utilisation pose a variety of challenges for service providers. They've started using encryption and key distribution as concepts for the protection and security of their clients' data.

Users of cloud computing want to know that their information will be kept separate from that of others. Otherwise, there is a possibility of data blending or mingling, which can cause insecurity or confusion. Cloud providers must give better and more consistent services to their clients as the demand for cloud computing develops. The infrastructure designs of existing cloud computing service providers differ from those of competitors. The safety and security of their clients' data should be the most important consideration for cloud computing service providers. They must think about how much security they want to integrate in the service without jeopardising their security system. Several significant companies have begun to employ cloud computing systems not just to store data, but also to analyse data using information technology, which can help any company expand. Cloud-based analytics include determining an individual's likes and dislikes, tracking systems used in online trade, and uncovering consumer preferences through tracing preferences.

INFORMATION SECURITY

The confidentiality (protecting private information from unauthorised individuals), availability (providing timely access to information to authorised users), and integrity (protecting the accuracy, reliability, and validity of data and databases) of information are the primary concerns of information security. Computer security also includes issues such as authentication (ensuring that people using the system are who they say they are) and nonrepudiation (ensuring that a legitimate user cannot deny using the system). Firms must also be able to detect and fix data security breaches after they occur. As a result, information security refers to a set of actions aimed at safeguarding data and information systems.

Despite efforts to prevent them, data security breaches are prevalent. The majority of research on preventing data breaches is technological, concentrating on issues like encryption and access controls. The research into the economic implications of information security, on the other hand, is limited but rising rapidly. However, little is known about the budgeting process for determining how much money to spend on information security. The costs of information security activities include a wide range of products such as hardware, software, and staff. Although most of these costs are best thought of as capital investments, businesses tend to regard them as operational expenses during the time they are incurred.

Budgeting for information security expenditures is a critical resource allocation choice, regardless of whether they are classified as capital or operational costs. From an economic standpoint, businesses should invest until the last dollar invested in information security generates a dollar in savings. To put it another way, information security investments should be weighed in terms of cost-benefit analysis. The cost-benefit analysis utilising the net present value (NPV) model is a well-established rational economic technique for budgeting capital investments. The risk-adjusted discounted present value of projected benefits and expected costs are estimated and compared in this method.

Although using risk-adjusted discounted cash flow approaches does not ensure better company performance, it does help firms allocate resources more efficiently. As a result, it seems natural for managers to budget for information security expenses using the NPV method. Unfortunately, totally rational economic cost-benefit analysis approaches (such as the NPV model) are rarely possible to utilise in budgeting for information security. Although predicted expenses associated with information security activities can typically be estimated with acceptable precision, the same cannot be said for expected benefits. Users must have information about potential losses from security breaches, as well as the likelihood of such breaches, in order to estimate the expected benefits.

The use of the NPV approach to determine an optimal expenditure level might be considered an ideal economic approach for budgeting information security costs. This technique is useful because it encourages companies to compare risk-adjusted expected benefits against predicted information security expenditures in monetary terms. Additional spending would be justified as long as the monetary value of the expected incremental benefits exceeded the extra expenditures.

Firms can use a modified economics approach to planned information security expenditures if they don't have access to this ideal approach. Managers, for example, may evaluate the projected potential benefits of preventing data security breaches without assessing the likelihood that such breaches would occur. Managers could also measure the likelihood of security breaches without measuring the expected cost as a result of those breaches. Another alternative is that both possible losses and the likelihood of such losses occurring are taken into account, but neither is quantified.

The management could compare the potential incremental benefits to the incremental expenses of information security actions in these scenarios. As a result of this intuitive comparison, the projected net return from such costs (the difference between the predicted benefits and costs) may be classified as high, medium, or low. Some managers may simply adjust the budget from the previous period to arrive at the budget for the following period's information security. As a result, an incremental budgeting method could be a major driver of information security spending. Managers may, on the other hand, perceive information security investments as must-do initiatives that must be completed regardless of cost-benefit analysis. This debate recommends two research questions that could be investigated in order to have a better understanding of how businesses plan (budget) for information security expenditures.

CONCLUSION

Data privacy refers to the appropriate use of data supplied to organisations for agreed-upon purposes. Customers' data should be adequate to meet their business requirements and wants; it should be accepted and supplied to them with full disclosure information. For failing to provide proper data privacy disclosure to clients, the Australian Federal Government continues to enforce penalties. Personal Identifiable Information (PII) is a term used to describe data collected in the banking and financial services industry. The confidentiality (protecting private information from unauthorised individuals), availability (providing timely access to information to authorised users), and integrity (protecting the accuracy, reliability, and validity of data and databases) of information are the primary concerns of information security. Cloud technology is a new upgrade for a more efficient processing system that uses the cloud as a warehouse to store data and make it easier to access when needed. This should be used in addition to manual data storing in our storage devices. Budgeting for information security expenditures is a critical resource allocation choice, regardless of whether they are classified as capital or operational costs. From an economic standpoint, businesses should invest until the last dollar invested in information security generates a dollar in savings. To put it another way, information security investments should be weighed in terms of cost-benefit analysis.

REFERENCES

1. Eling, Martin, and Werner Schnell. 2016. "What Do We Know About Cyber Risk and Cyber Risk Insurance?" Journal of Risk Finance 17 (5): 474–91.
2. Gordon, Lawrence A., Martin P. Loeb, and Tashfeen Sohail. 2003. "A Framework for Using Insurance for Cyber-Risk Management." Communications of the ACM 46 (3): 81–85.
3. Hunziker, Stefan. 2021. Enterprise Risk Management: Modern Approaches to Balancing Risk and Reward. Springer Nature.
4. Kendrick, Rupert. 2010. Cyber Risks for Business Professionals: A Management Guide. IT Governance Ltd.
5. Korstanje, and Maximiliano E. 2016. Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities. IGI Global.
6. Leuprecht, Christian, David B. Skillicorn, and Victoria E. Tait. 2016. "Beyond the Castle Model of Cyber-Risk and Cyber-Security." Government Information Quarterly 33 (2): 250–57.
7. McQueen, Miles A., Wayne F. Boyer, Mark A. Flynn, and George A. Beitel. 2006. "Time-to-Compromise Model for Cyber Risk Reduction Estimation." In Quality of Protection, 49–64. Springer US.
8. Nagaraju, Vidhyashree, Lance Fiondella, and Thierry Wandji. 2017. "A Survey of Fault and Attack Tree Modeling and Analysis for Cyber Risk Management." In 2017 IEEE International Symposium on Technologies for Homeland Security (HST), 1–6. ieeexplore.ieee.org.
9. Radanliev, Petar, David Charles De Roure, Razvan Nicolescu, Michael Huth, Rafael Mantilla Montalvo, Stacy Cannady, and Peter Burnap. 2018. "Future Developments in Cyber Risk Assessment for the Internet of Things." Computers in Industry 102 (November): 14–22.