

Accounting information system

[Business](#), [Accounting](#)



" Companies should be held liable for losses sustained in a successful attack made on their AIS by outside sources."

Accounting Information System (AIS) “ combines the study and practice of accounting with the design, implementation, and monitoring of information systems.” With recent technological developments, modern information systems combined with traditional accounting controls and methods provide users the financial information needed to manage organizations faster and more efficiently.

The major challenge that recently faces companies is the security of the information derived from their information systems against unauthorized users or outside sources. According to Beard and Wen (2007):

“ The use of Internet technologies has substantially increased the vulnerability of information systems. One of the fastest-growing threats on the Internet is the theft of sensitive financial data. Failure to include basic information security unwittingly creates significant business and professional risks.” (p. 1)

For effective implementation of AIS, it must have provisions for controls. “ The AIS should provide adequate controls to ensure reliability and accuracy of financial data to safeguard assets and minimize errors and fraud.” (Cabrera, 2006) In the research of Laurie Henry, 44% of the loss of accounting information with the new technology is caused through malware malfunction and theft. (cited in Ontracks Computer, 1996) As presented in the survey results made by Laurie Henry presents that as a business earns

more revenue, it is more likely to have a highly computerized accounting system (85.5 percent). (1997, p. 3)

It was also noted in the research that companies reported suffering losses due to either employee actions or due to the actions of an outsider were outsider losses range from less than one half million dollars to five million dollars in revenues annually. “ Further review of the nature of the accounting system hardware in the outsider losses shows one business utilizes a network and one utilizes a client/server system.” (Henry, 1997, p. 6)

The conclusion established in the research study suggests that there is inattention to security methods over computerized accounting systems by organizations for absence of full awareness of the availability of possible security methods; such costs will not be outweighed by benefits; “ and/or they are indifferent to the need for security in automated systems until a loss occurs.” (Henry, 1997, p. 17)

As shown in the study, companies are still not utilizing and optimizing available security measures to protect their financial information from outside sources. As such, companies must still be held liable for losses sustained in a successful attack made on their AIS by outside sources in the absence of “ adherence to standards for software design and development as well as standards for control of information technology.” (e-notes. com, p. 1)

Implementation of basic simple securities such as virus protection, password access, backup of data and periodic audits may provide at least some assurance that accounting data will not be lost or corrupted. Computer

networks are susceptible to high level risk which requires special controls and security measures. “ The responsibility for establishing and maintaining a system of effective internal controls resides with management.

Management’s responsibilities include the documentation, testing, and assessment of internal controls, including relevant general IT controls and appropriate application-level controls designed to ensure that financial information generated from an organization’s information system can be reasonably relied upon.” (Beard and Wen, 2007, p. 1) Companies must invest not only in the implementation of these security measures required but also in meeting minimum standards of the level of security and control in order to ensure protection of its financial information against outside sources.

Establishment of accounting information system carries with it the security risks involved in its safeguard which organizations must be aware of and respond to. Failure to comply with the minimum standards will result to possible unauthorized access over financial information were they must be made accountable. Companies must eliminate these threats on the onset since it will be open to potential risks of successful attacks by outside users. It is not enough that securities and controls are established but standards must also be met to comply with company objectives in the safeguard of its vital asset, which is information. Securities and controls maintenance and periodic audit must also be observed.

It is important to note that most companies, if not all, are indeed aware of the threats presented by technological advancements and the utilization of the Internet which are indispensable in its business operations. Nonetheless, awareness does not usually address to the necessary level of reactions that

must be confronted by these companies to optimize the security of their accounting information system against these present and on-going threats. Accountability of the companies for losses sustained from these threats must still be properly dealt with since they are primarily and continuously responsible for safeguarding their accounting information system against any form of security breaches.

References

Beard, Deborah & Wen, Joseph H. (2007). Reducing the Threat Levels for Accounting Information Systems Challenges for Management, Accountants, Auditors, and Academicians. Retrieved from <http://www.nysscpa.org/cpajournal/2007/507/essentials/p34.htm>

Cabrera, M. E. (2006). *Management consultancy principles and engagement* .

C. M. Recto: GIC.

Henry, Laurie (1997). A study of the nature and security of accounting information systems: the case of Hampton Roads, Virginia. Retrieved from <http://www.allbusiness.com/accounting/656483-1.html>

<http://e-articles.info/e/a/title/ACCOUNTING-INFORMATION-SYSTEMS/>

<http://www.enotes.com/business-finance-encyclopedia/accounting-information-systems>