The myth of secure computing by austin and christopher

Digital security is gaining importance nowadays as all business processing is shifted to a computerized setup. Austin and Christopher in their article, “ The Myth of Secure Computing” (2003), inform about the state of digital security in companies nowadays. Digital security is given least importance in any business setup ignoring the fact that every year companies face heavy financial losses on the basis of security breaches. Austin and Christopher inform that companies have developed networks for their day-to-day processing and separate IT departments with IT heads are there to control any kind of digital issues. However, the amount of money spent on digital security is only 5 to 10 percent of a company’s total expenditure due to which, there are risky security concerns.

There are many threats to digital security, which are as follows:

Network Attacks, which are responsible for slowing network functions and disrupting online performance, are common threats to digital security that can result in big financial losses for the company. Network attacks are external.

Intrusions are internal attacks and are more dangerous than network attacks as the intruders can use the same rights to alter or damage data as authorized users. Intrusions can cause not only monetary but also data leakage loss.

Malicious Codes are in form of viruses and worms that keep the capacity of destructing a company’s whole network. Company’s data can be erased wholly because of viruses and worms.

All kinds of threats are highly dangerous and need to be analyzed in advance. The IT department of a company needs to be highly efficient in identifying all kinds of threats and the level of security that should be provided to each and every asset. An operational approach needs to be followed in order to secure the company, its assets and its reputation from any digital security breach. Risk management should be there in order to check the possible risks to a company's digital security and to control them in time.

The IT department is required to keep continuous check to day-to-day processing. If software programs are used in a company, they must be tested regularly. The coding, testing and implementation process should not be conducted with proper care and efficiency. The IT staff should be well equipped with all concerned knowledge about IT state of the company and required security measures.

The writers of the article have pointed towards a crucial issue that needs attention to detail. The companies working today are computerized mostly and have their own networks due to which, they are in need of digital security measures so that they face minimum security breaches and can control any intrusion in order to save them from big losses. The article is an affective write-up and needs attention.

References

Austin, Robert D. and Christopher, A. R. (June 2003). The Myth of Secure Computing. Harvard Business Review 81 (6)