Citibank data, that would have reduced any capital

Finance, Banks

Citibankis one of the largest and oldest banks that has been offering services to itscustomers. Incidents can be prevented most of the times by taking correctsafety actions and imagining the worst and all kinds of situations possible. Fromthe incident it is evident that a suitable and necessary plan to mitigate theoverall, loss was missing or weak.

Identifying risks is a significant step, followedby prioritizing the risks. These are to be thought in all possible ways toprevent such incidents. Theincident of 2005 could have been prevented by the bank up to some extent byminimizing the quantifiable breach of data or the nature of loss. Any bankwould not want a bad reputation for itself to be able to do business with thepeople. More than the corporate culture of Citibank, it seems due to the lackof foresight and safeguard ideas to protect the data, that this incident hashappened. Citibankwas one of the first banks to introduce Automatic teller machines(ATMs), giveonline access to customers to their accounts through dial-up and later throughbrowser. Considering the technological advancements and adaptations of the bankin the not-so-known time of the technology, bank could have adapted clever waysof storing information of the customers.

Citibankshould have opted for cloud storage and invested in its development which wouldhave avoided physical theft of the tapes. IfCitibank used cloud to store data, that would have reduced any capital expensesand the data can serve as backup in case of disasters. Besides the mediastorage, if explained extensively to the world, it would have garneredattention from the people thus gaining more customers. IfI was the CSO of Citibank, I would have invested in the cloud storage and itssecurity rather than the tapes, which is quite different from other banks incompetition. Butowing to the fact that cloud storage was not so developed at the time of thisincident, steps should have been taken to start using the cloud and focus onthe security while transmitting data and also while storing because sensitivedata in transit can cause data breaches. Also, below are some of the steps that can be taken while storing data ondisks/tapes.

·   Usinga strong encryption method while storing data on physicals devices, ·   Maintainingduplicates of the information, ·   Keepingthe private key that can be changed at any time remotely during transit ofdevices, ·   Devicinga plan that can destroy/corrupt the attacked copy of data,·   Triggeringa mail/message to concerned parties immediately after the data is compromisedand ·   Storingthe devices in strong locker rooms which are difficult to invade ·   Fixingthe routes without any prior plans on which the data can be transferred·   maintainingsecrecy about the transit of media and·   Conductinga patrol in the area beforehand for any threats during the transit. Aneffective CSIRT team is essential in such cases of data breach. A rapid andaccurate target can minimize the financial damages which are caused by theincident.

Assuming we have steps to be taken in case the data is compromised, CSIRT team should try to change the nature of data by modifying the dataencryption or corrupting the data as a final steps, if the data is getting intoevil hands and cause some serious threats to the persons involved. Ibelieve the steps taken are ample as they do not have leaks and are thoughtwell in all possible ways.