Impact of cyber-crime

Business

Attacks on computers may acquire different forms, like malware, worms, and attacks on DOS, viruses, and use of other malicious software that aims at destroying and/or damaging a computerized system. If a computer system is affected by malware, an institution risks serious financial, reputation loses or even closure. This is due to the colossal damages incurred by attacks. Cyber criminals, among them hackers, are a threat to the financial institutions worldwide. The financial institution CITIGROUP's lately suffered cyber attack.

Information regarding 360000 credit cards was stolen from the institution's internal server. The financial institution was just another target after other large firms, like Sony Corporation andGoogle. It's quite clear that CITI has no control over what sites their customers may visit when using the internet. However, if the customers' information is stolen, the institution will be negatively affected in several ways.

The public and the customers of CITIGROUP banks may lose faith and ultimately goodwill in the banking security and its performance. This translates to customers shifting to other financial institutions for their banking services. Huge amounts of revenue disappear in the process as customers reduce. Some of the programs are completely damaged, which calls for fresh installations. This process is costly to the institution, and adds to the already long list of expenses.

The institution also has to put up counter-measures. This process requires hiring new staff, and buying new computer software increasing the budget. A failure in Citigroup's operational systems or infrastructure, or those of third parties, could impair its liquidity, disrupt its businesses, result in the

disclosure of confidential information, damage Citigroup’s reputation and cause losses. Attribution or a trace-back action is mainly performed to acquire a source and probably the responsible culprit. This happens during or after a cyber attack.

Attribution is an organized process of tracing back to try and determine the identity of the source of a cyber attack. There exists two types of attribution; digital identity (computer, user account, Internet Protocol (IP) address, or enabling software) and physical identity (real person). There’s a need to educate people, particularly internet users, on the correct acceptable use and code of ethics. Cyber ethics refers to a system of safe and responsible behavior mostly for internet users. CITI follows a strict policy on code of ethics that embodies common purpose, responsible finance, leadership and team work.

To minimize threats brought about by cyber attacks, CITI has to employ a number of policies and strategies to implement protective programs. CITI employs the multifactor authentication policy as required by the FFIEC. The process uses hardware tokens with dynamic PIN generation and also the use of a one-time password. In addition, regulatory guidance demands multiple or several levels of authentication for bank clients that use the banking services online. CITI’s policy requires use of industry-accepted security practices, including firewalls and encryption.

These security controls allows proper authenticity of a customer’s identity when they access online services and help to protect the information as it travels online. Other policies to safeguard users account include; secure

login, cap on number of login attempts, timed logout, user ID expiry, 2048 bit secure socket layer and also collaborate with entrust digital certificate. Other security policies like Phone-based authentication allow direct communication with the customer thus increasing security.