Security measures essay sample

Law, Security

When it comes to security and the protection of proprietary and sensitive information, there can be no excuse to not have the best available safeguards in place. Security breaches come in many different shapes and sizes. They can be orchestrated by massive units that aim at breaching sensitive information hubs and leaking that information to the public. An example of a malicious attack would be one committed by the group Anonymous. Defined as " any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanism", (Techopedia), a security breach can be internal or external. " Depending on the nature of the incident, a security breach can be anything from low-risk to highly critical", (Techopedia). Both types of breaches can be just as dangerous and costly and affect a company in the same negative fashion, whether it be an accidental breach or a malicious attack. And both require extensive security measures to protect a company from such breaches.

There are numerous security measures that are already set in place and implemented at First Republic. When we break down the different levels of security, there are numerous fields that utilize different security measures. On the employee level there are absolutely no non-employees allowed on the floors on the Corporate Office. For an employee to gain access they have to wear two identity badges that also serve as their elevator pass and their door pass to their assigned floors. For personal privacy each employee has a desk with two drawers that lock that they are required to keep their personal belongings in and lock when away from their desk. When an employee is hired they are required to sign an addendum to the application stating that they will never divulge any internal information of FRB to anyone ever.

There are severe auditing rules and a strict structure of completion that we pride ourselves on as we are dealing with finances of individuals and companies. FRB has multiple contingency plans in place for each location in the event of a natural disaster or a catastrophe that limits the ability to work from our Corporate Headquarters. The most important safety measure that is employed on a daily basis is the computer software/network protection run by the IT department. It is essential in the line of work that FRB is in that all its devices are equipped with the top of the line anti-virus/hacking protection available. The typical security problems that could arise at FRB are persons attempting to gain access to unauthorized locations.

Or the constant threat of information being leaked or hacked via computer fraud. The control procedures that are already in place are that each and every email that is sent out from an FRB employee is automatically encrypted and the receiver has to navigate to a link via the email to retrieve their information. The ethical dilemmas that are faced when employing certain control mechanisms are that you can’t please everyone. There will always be someone who is negatively affected by a decision and the implementation of that decision. The recommendations that I have are that FRB needs to continue to pursue all forms of computer safety in regards to protecting the gathering and the flow of all internal and external information.

References

Security Breach. Techopedia. Retrieved 06/05/2013 from http://www. techopedia. com/definition/29060/security-breach