Hacking will impact your businesses

The recent hacking of the website of the Commission on Election (COMELEC) and the computer systems of the various banks and companies raises concern on the reliability of the elections and the security of sensitive business information. This becomes of utmost concerns especially since hat the suspected COMELEC website hacker is neither an experienced professional nor a group of IT experts but a 23-year old fresh-graduate individual.

Hacking is the way of gaining unauthorized access to data in a system. This is a serious issue since in this digital age, companies are dependent on Information Technology (IT) infrastructure in storing, processing, planning, scheduling, and transmitting not only information but also resources or funds.

Clearly there is the need to secure data of companies from unwanted access. Companies spend large sums on employing capable IT Administrators, backing up facilities, installing anti-virus programs and formulating of company policies to ensure that no confidential information will leak or no hazards will flow inside the IT system.

Hacking, no matter what the intention is, causes disturbance in a company's operations. After a hacking episode, restoring or re-connecting the system to its normal operation is not only expensive but requires time and attention. Moreover, the losses arising from hacking is difficult to measure in terms of monetary value.

Imagine the impact of hacking on online retail stores. These will temporarily be inaccessible because of the interference of hackers. The delay definitely will result in decline in sales resulting from potential customers unable to proceed with their intended purchases.

Hackers are not just doing their activities for fun or self-fulfillment. They can do more drastic thing that can affect a lot of damage to the company. Companies that are hacked lose their integrity and the trust of their stakeholders that may result not only to closure of the business but may also attract lawsuits from the public because of the confidential and personal information that these companies fail to secure. Hackers may not be able to steal the data in the system but they can make the information unreliable thru alteration and deletion of data.

A hacker can expose researches, trade secrets and formulas and even financial reports of companies. Once hacked, the competitive the hacked companies , the security of its customers list and other areas of its operations will be adversely affected. Information such as the names, addresses, contact numbers, bank account information, specimen signatures and the electronic copies of identification cards are just some of the data in the database. When these data are captured, it can be used for illegal activities, such as identity theft, unauthorized bank withdrawals and even in making loan application under the name of another person. Hackers can also profit from the hacked information such as client lists, trade secrets and researches by selling these to interested persons.

Although the Republic Act 10175 (Cyber Prevention Act of 2012) provides for sanctions to offenders with penalty up to 10,000,000, this may not be sufficient to deter cyber crime.

We must stay alert to prevent hacking and other cyber crimes. The recent hacking of the COMELEC website, the cyber theft of the deposit of the Bangladesh bank , the many phishing of bank accounts and many other related incidents are testimonies that cyber crimes are threats that can happen any time

Prevention is better than cure. Communicate to management or the I.T. in-charge of irregularities, issues or any occurrences that you may encounter. Include possible cyber-attacks issues in the disaster recovery plans of companies. Basic preventive activities can be put in place including , the regular update anti-virus software, installation of firewalls, strengthening of security by not allowing personal laptops or any devices that can copy and store information, blocking websites that may be used as a channel to connect

to the system, refraining employees from using personal email account when making transactions or transmitting information, and others.

Jeffrey Galang Salazar is a Certified Public Accountant and Master in Business Administration degree holder. He is currently connected with Tong Hsing Electronics Phils Inc., Mold Parts Manufacturing Asia Inc. and Pamantasan ng Cabuyao.

This column accepts contributions from accountants, especially articles that are of interest to the accountancy profession, in particular, and to the business community, in general. These can be e-mailed to boa.secretariat.@gmail.com