Inside this Issue Vol 1: issue 3/16

Cyber Tips

How to stay safe on line.

Cybercriminals have become quite savvy in their attempts to lure people in and get you to click on a link or open an attachment.**Read more >>**

Types of cyber attacks

For the most part unavoidable,companies have found ways to counter cyber attacks using a variety of security measures. Regardless how safe a business feels its systems are, everyone must still be aware of and vigilant towards online threats.**>>**

Institute Of Forensics And Ict Security www.forensicsinstitute.org

Forensics & Cyber Security Newsletter

Your source of forensics, security and fraud insights

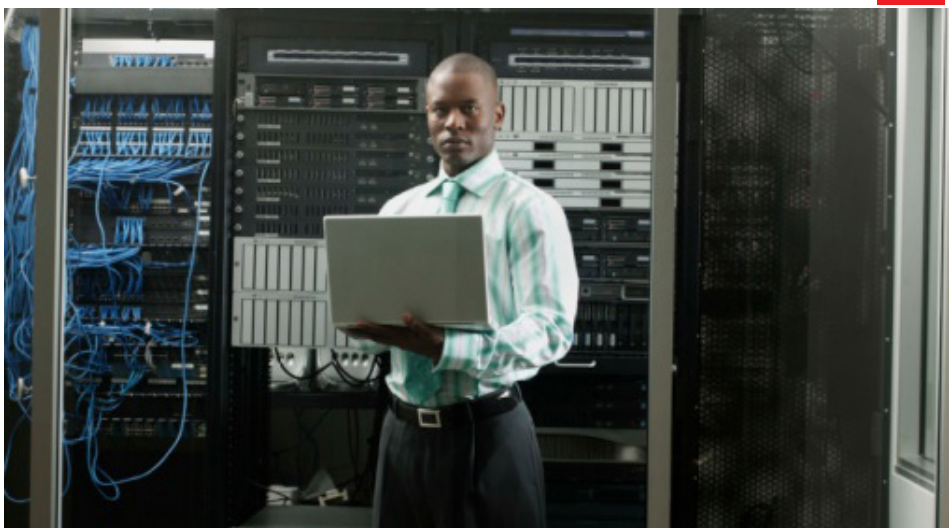
Sept. 2016 | Vol4 / free

Student of the Month

The Institute of Forensics has helped me know that there are professionals that are helping in fighting fraud. They help detect and deter fraud related cases. As a result of the Institute I have been able to get in touch with the International world by attending ACFE international workshops, as a CFE I also receive a monthly newsletter from the international body of the Association of Certified Fraud Examiners.

The environment at the Institute was so favorable and it enabled me to concentrate and pass the exam. I strongly encourage and recommend any one that would love to take on CFE to enroll for it at the Institute of Forensics and ICT Security.

Sauda Namuleme, CFE



Secure the confidentiality of your data

Are you secure on line?

You cannot solve a problem by running from it. Yet, this is what most top honchos and senior IT managers in most businesses in Uganda are doing: refuse to accept that cybercrime is a problem that needs urgent attention.

Now is the time to recognize the problem of cyber-attacks. Banks must not only invest in anti-fraud technologies especially firewalls like SIEM – security information and event management and NAC– network access controls, but human defense. The fact is there is no patch for human stupidity. However, up-to-date your systems are, if your users (staff and executive) are not security conscious, they present the weakest defense to your security setup.

By far, poor IT governance especially in the areas of change management, backup, security consciousness and first response practices following an attack, are some of the major challenges experienced.

One of the reasons for the increasing cybercrime incident is that cyber criminals are taught to be more technically advanced than the internal bank staff that

To page 2

From page 1

plan to thwart or prevent them. A cybercriminal is more persistent than ever. And thanks to the advanced global community of hackers with great resources on advanced system security breaches and penetration, identifying a target and starting an attack is easy. On a website like, https://cve.mitre.org/ a bad guy can easily find attacks like zero day exploits – these are exploits that have recently been identified by hackers on any commonly used system which could be an off-the-shelf international banking application but which the vendor is yet to find a patch to fix and send to all her customers to update.

Such zero day exploits, in the hands of a motivated hacker, could easily wreak havoc especially if the target staff are not security conscious. A security breach involves loss of confidentiality, integrity and availability.

If you are a mobile money or bank customer, you have probably visited a bank and they told you to wait a little, as the system is off. In that case, the bank is experiencing a security breach and failing to provide system availability, which should always be on at 99.9% for a well-managed institution or not less than 90% of the time. If you have had to go back to the bank and complain about some deductions on your bank balance which you are not aware of, that is loss of integrity. Your bank account should only be debited or credited with your approval and nothing else. And if you find some you did not expect to know your bank balances or the different accounts you have in a bank that could be a red flag of loss of confidentiality. The bank owes you a duty to secure your data.

The recent case of Yahoo breach, http://www.usatoday.com/story/tech/2016/09/22/report-yahoo-may-confirm-massive-data-breach/90824934/, is one of the lapses in cyber security. As you can see, cyber security breaches could lead to business collapse. And that is another reason cyber security is a business of the board and top management.

Why our Society has increased the level of corruption and frauds in our Country

We live in a country where society measures your level of success based on how much property you own, which type of car you drive, even including the schools where you take your children. We have been made to believe that you can only be successful if you are seen to be successful irrespective of what troubles you go through to keep up the appearances.

My recent visit to my village proved to be the most expensive trip in my life. Once you have gone to school and gotten a job, most relatives and other village neighbors want a piece of your so called success. They will tell you stories of how climate has changed and they no longer harvest enough for food, how they have been unlucky with their children going to school and no jobs,

Everybody who knows or has ever heard of your name will come to ask for something, from money for alcohol, food, school fees, jobs for their children and grand children, etc. These people expect you to be successful. Nobody will give you the respect you need unless you are driving a car, they don't mind to inquire whether it's borrowed, hired or a company vehicle. If you don't give any money, some will go ahead to tell you how they contributed to your being successful, or even how they wished the money you have and don't want to give could change hands and you be like them.

Even in our churches, when you go to attend service is when the priest will remember how the church has not been painted, local worshippers will bring items for auction and then hike the prices anticipating that you will finally take the item, and you have no option to keep quiet or leave before the service ends. Others will start buying small items for you or your children if you have moved with them to church, this makes you look small if you cannot buy anything for yourself or for another worshiper. Of course not forgetting the basket collections for either a local going for priesthood or a church's anniversary, there has to be something to contribute to. With the fear of witchcraft and bad omens, you end up emptying your pockets and driving back on an empty fuel tank.

> ***This society has made us want to look successful to be appreciated and nobody minds how you acquired your success***

This society has made us want to look successful to be appreciated and nobody minds how you acquired your success. Some people will go ahead to praise robbers for as long as they feel these contribute to their survival irrespective the form of survival. I have friends and relatives who have come up openly to search for particular jobs that will expose them to lots of cash in terms of kickbacks and other hand outs because they want to make a lot of money. Others have expressed fear of visiting their villages without vehicles or wearing something new and unique. All these money desires lead to corruption and frauds.

We no longer consider humble beginnings and humble livings, not when people feel they are being

Kickbacks in the Health Care Industry

With media reports about the government health care breakdown in Uganda, there has been an increasing number of private health care units to take advantage of the population that can afford to pay for health care services. But as any other sector in Uganda, it has not been spared of corruption and other scandals. In this issue, we discuss the most common fraud schemes in the health sector – Kickbacks.

Kickbacks in the health care industry can come from several sources. The medical community is facing competition that it has not faced in the past, and monetary offers to prospective patients have been difficult to refuse. Examples of kickbacks are:

The most common one in Uganda is a doctor referring you to particular specialists.

- Payment for referral of patients
- Payment for vendor contracts
- Waiver of deductible and copayments
- Payment for insurance contracts or health care programs
- Payment to Adjusters

a)Payment for Referral of Patients

Providers in an area of high competition will pay "runners" to recruit new patients. In addition, patients may receive a monetary reward if they refer another patient to a provider. The provider makes up for the kickback in the unnecessary billing of medical expenses or false claims. In addition, providers will pay kickbacks to other physicians for patient referrals. The most common one in Uganda is a doctor referring you to particular specialists.

b)Payment for Vendor Contracts

Companies doing business with medical practitioners will pay a "consulting" fee for referring business to them or using their supplies. This is common in nutrition supplements especially for pregnant women and infants. We have witnessed several incidences where sales persons are always in the queue to see a Pediatrician or Gynecologist carrying heavy bags. As soon as the patient enters, some of the medicines are still on their desks and are the same that the doctor will recommend for you.

c) Waiver of Deductibles and Copayments

Many health care programs require patients to pay a deductible and copayment, or a small portion of the total payment, for services rendered. One of the reasons for having copayments is to make beneficiaries take an active part in the financial responsibility for their care. To attract patients, however, providers might improperly pay for or waive the patient's out-of-pocket expense, hoping to make up for that cost in additional business.

d)Payment for Insurance Contracts

Physicians with patients who are facing long-term care or lifetime treatment, such as dialysis for kidney failure, might purchase additional insurance contracts for their patients. This ensures that the provider will be paid, and the patient has no out-of-pocket expense.

e)Payments to Adjusters

In order to get a claim settled quickly, a beneficiary, or someone operating on his behalf, might bribe adjusters or other claims-handling personnel to approve or speed up the payment of a claim to a health care program.

From page 2

left out on "living life". But if we are to reevaluate ourselves again and teach morals straight from grassroots, our society can return back to where we were before.

We cannot deny that society has increased the level of corruption in our country. We can only go back and encourage and support our people to focus on agriculture and other activities to be able to generate their own income. We can also slowly re-emphasize morals right from childhood but above all be able to punish whoever gets involved in corruption and frauds.

Acquire practical skills to fight against corruption

Types of cyber attacks

The success of a spear phishing attack is dependent on an end user clicking on a link embedded in a crafty email.

Our experience shows that most attacks are either insider or external. Insider or internal attacks involves breach of trust from employees, consultants, vendors, or other partners within an organization. Most notable cases in Uganda involving cyber breaches have been perpetuated by former employees working with some insiders they left behind or software vendors who are often called to provide fixes. For the latter, experience shows that bank staff must be trained to acquire the skills to maintain and do fixes to the core banking application other than relying on the vendor.
It is not good idea for a vendor to come and effect the patch upgrade to a live system.

The best practice would be that the upgrade patch is provided to the bank's IT staff who then test the patch on a separate environment, preferably a bank's own sandbox so as to see the impact of the patch on the system. And after satisfying themselves, the patch can be applied to the live system. Most of the frauds in Ugandan banks are due to the reluctance of the bank to have clear agreements with the vendor in respect to know-how transfer so that the internal bank staff are empowered to maintain the core application. Many banks rely on outsiders by most part, which is very regrettable.

External attacks involve hackers hired by either an insider or an external entity whose aim is to destroy a competitor's reputation.

In the next issues, we look at specific cybercrime cases and the steps involved in forensic investigation. To learn more, visit **www.forensicsinstitute.org**

Cyber Tips

continuation...

7. Protect Your Children Online

Discuss and set guidelines and rules for computer use with your child. Post these rules by the computer as a reminder. Familiarize yourself with your child's online activities and maintain a dialogue with your child about what applications they are using. Consider using parental control tools that are provided by some Internet Service Providers and available for purchase as separate software packages.

8. Protect Your Portable Devices

It is important to make sure you secure your portable devices to protect both the device and the information contained on the device. Always establish a password on all devices. If your device has Bluetooth functionality and it's not used, check to be sure this setting is disabled. Some devices have Bluetooth-enabled by default. If the Bluetooth functionality is used, be sure to change the default password for connecting to a Bluetooth enabled device. Encrypt data and data transmissions whenever possible

To be continued....

4th Floor, Ntinda Complex, Plot 33
Ntinda Road opp. St. Luke COU
P.O Box 40292, Kampala, Uganda

T. +256 414231136/ +256 393517236
E. admissions@forensicsinstitute.org
aamumpaire@summitcl.com

visit our website for more information
www.forensicsinstitute.org
www.summitcl.com

Send your comment on the articles or any contributions to risk@summitcl.com

The Institute of Forensics & ICT Security (IFIS) is training arm of Summit Consulting Ltd. We offer digital forensics, advisory and ICT Security

summit consulting