Banking security case

Law, Security

1) Reasons for not reporting the threat to the police

Great challenge

Could be the first manager suggested not involving the police because this was the best way to avoid facing shame of admitting that a particular bank had been hacked. On the other hand, the manager is aware that law enforcement has experienced great challenges particularly because of the issue of computer crime and hence the police would face much difficulty to address the problem. The lawbreakers have with them highly incorporated technical methods and come with creative ways of executing the crimes.

They complicate investigation by crossing state as well as national boundaries. Furthermore the evidence of computer crimes is neither human nor physical but if there is, it is based on programming codes and electronic impulses. Unfortunately, the police are much behind the computer age and it would take centuries for them to understand some of the terms involved in computer crime. To make it worse, it is difficult for police to comprehend and belief computer crime is a major problem that has a local impact, despite of the location or size of their communities (Carr & Williams, 2005).

Inadequacy of resources and equipments

The law enforcement lack propereducationthat is related to computertechnologycrimes. The law enforcement has concentrated more on violent crimes hence placing the computer crimes in a low priority status, forgetting that loss that comes with computer crime could result to a major downfall for the country. It means therefore that the law enforcement has inadequate equipments and resources for dealing with computer crime.

Many crimes that makes use of computer technology matches with the traditional offenses like fraud or theft and the technical complexity, creative avenues and speed by which the crimes happen pose specific problems to detection, prevention as well as prosecution (Carter & Katz, 2010).

Offenders not adequately prosecuted

Research has revealed that if computer crimes are reported to police, they do not hold a high probability of being prosecuted. As stated above law enforcement lack proper resources for dealing with such crimes as they have placed higher priorities to other crimes. The nature of the menace which computer crime poses to banks is greater than it is imagined. There is a massive technological change and despite of the fact that in UK there are laws that have been framed in general terms so as to address the current offences, the legislation continue to lag behind because of the speed at which the technology is evolving.

Looking back into history, the UK legislation developed the Computer Misuse Act in 1990. The act was developed to address the growing concern that by that time, the legislation was not adequate in addressing the computer crime (Emm, 2009). In1984, Robert Schifreen and Stephen Gold who had gained unauthorized entry to BT’s Prestel service were never convicted under the act.

Though the individuals were charged under the 1981 Forgery and Counterfeiting Act, this was done after many years. This reveals that the legislation is too slow to prosecute individuals who have committed

computer crime and therefore reporting the threat to the police, the banks would have to wait for a lengthy period of time for their case to be heard

Again after the creation of the Computer Misuse Act in 1990, the first prosecution came after five years and this involved an individual who was allegedly charged for distributing a computer virus. The individual pleaded guilty of the crime and as a result received a prison sentence for 18 months. The damage caused by this individual cannot be compared to the sentence that he received at last.

This shows that even if the banks report their threats to the police and suspects get arrested, probably they will not receive the punishment they deserve for their crime. Such suspects should receive severe punishment for their crimes because the damage they commit is sometimes irreversible and immense (Carter & Katz, 2010).

The Police and Justice Act that was formed in 2006 offers under section 1 that the maximum prison sentence an individual can receive is two years. The section has been posed with a lot of criticism from people mainly because of the period prison sentence. Many people still hope that this section will later on be amended and this means that before the amendments, there will be a lot of injustice especially to the banks.

It is not easy for the police to offer adequate prove that a certain person executed a computer crime and declaring one guilty of such a crime is equally hard. Hence this offers one of the reasons why the first manager opted for solving the issues entirely than involving the police.

Police not trained

Following the formation of the Computer Misuse Act, there were very few police authorities in the UK who were outside the Metropolitan Police area had expertise and knowledge to deal with computer crime. Though there have been concerns of addressing the problem, there is still inadequacy in addressing sensitive issues that concern computer crime.

According to a certain report on computer crime there is just one police out of four who can generate records concerning e-crime and this shows that a large proportion of suspects go undetected. Basing on the report, this problem is hampering prevention while at the same time distorting crime figures. Not every police have forensic computer training, which is one of the requirements in detecting crimes today as most of them contain digital element. According to the report, the computer crime training is available for all officers but only a few turn up for the training (Young, 2006).

2) Advantages of not involving the police

In the current world, there is great concern on thefailureof criminal justice system in addressing the threat posed by computer crimes in the banks. This is so immense in the banks where computers are infected with worms and virus while at the same time the systems end up being corrupted in different ways.

From previous reported cases regarding issues to do with computer crime, individuals who have been reported after being involved in computer crime have not received the punishment they deserve. For instance, out of the 61000 authors of malicious programs, only five of them have been arrested

and convicted. Of those arrested, only one author of Pathogen virus has received heavy punishment while the rest were under very light punishment.

This part of history shows that, even if the bank managers report their cases to the police, they might not get sufficient help. They would rather think of other ways of solving their problem rather than waste time andmoneyin trying to seek help from the police. Failing to seek help from the police therefore will save the bank managers the frustrations and embarrassment they are likely to receive from the criminal justice system. Moreover, the police have been assumed to hide records concerning computer crime and therefore if the bank managers report their cases to the police, they may be not be heard or dealt with in future (Walden, 2007).

Disadvantages for not involving the police

It had been stated earlier that it is hard to detect traces of computer crime as the evidence is based on programming codes and electronic impulses. This means that no human or physical evidence may be found after the crime. Despite of this, the police are currently being offered an opportunity of training in forensic computing and even though not all of them are trained in the field, those who have acquired the knowledge may help greatly in dealing with issues to do with computer crime. Failing to report their threat to the police, the bank managers could be missing an opportunity of encountering with a police with adequate knowledge or understanding of computer crime (Johnson, 2005).

Probably, the trained police would use their knowledge and investigate and consequently get hold of the suspects. Though the suspect may not receive

the proper punishment as required, the police may help the bank in revealing sensitive data concerning the crime. Moreover, if it happens that the suspect is finally caught, definitely he will receive punishment and be kept under close scrutiny to avoid the recurrence of related crimes from the same person. From this point of view, the banks could be given some enlightenment concerning the prevention of computer crimes (Johnson, 2005).

Police in UK have been known to consider computer crime as a minor problem that has little impact on the community. This has made them to concentrate more on other crimes such as drug trafficking, prohibition and violent crime among others while neglecting computer crime. On the contrary, computer crime is a major problem that continues to negatively affect the banks in not only United Kingdom but also in other parts of the world. If the bank managers fail to report their problem concerning threats to computer crime to the police, then the mentality held by the police will remain.

The police will never realize that computer crime is a serious crime that needs much attention just like other serious crimes. It therefore means that the law enforcement will never impose laws that could lead to the reduction or prevention of computer crime. On the contrary, the banks would continue suffering in the hands of hackers who even if they are caught they are not dealt with as it should be. Failing to report the threat to the police would limit more research that could be carried out around the country that possibly would produce findings relevant in addressing the issue in a more critical perspective (Casey, 2004).

3) Advantages of using hackers to test the bank security system

Hackers have technical knowledge

The types of hackers who are programmers are capable of finding vulnerabilities in existing code. They are hackers who are well educated and hold a deep understanding regarding computer technology. They are capable of developing a particular program to correct a vulnerable program in the computer system. This means that the technical knowledge that the hackers have can be very beneficial to the bank. If hackers are hired to guard the security system of the banks, they may even teach security professionals on how to hack so that they can protect their own system (Hatch et al, 2001).

Since many hackers are known to be self-taught prodigies they can be employed in the banks as part of the technical support staff. In this situation they will apply their skills and find flaws to the security system of the bank and hence they are repaired very fast. This type of computer hacking in most times assists in preventing identity theft along with other serious crimes related to computer.

Hacking results to technological developments

Computer hacking in banks can result to constructive technological developments. This is because many skills that are generated from hacking can be applied to many mainstream pursuits. For instance, UNIX operating system was developed in 1970s by former hackers Ken Thompson and Dennis Ritchie. This system contributed a lot to the development of Linux which is a free UNIX form operating system. Another example is that of

Shawn Fanning who generated the Napster and these two examples illustrates that in the process of involving hackers to inspect the security system of the banks, further developments in the technology can be made.

This ultimately will lead to a lot of benefits to not only the banks but to the entire world at large. However, this can be accomplished if the banks happen to hire the ethical hackers. With these types of hackers, the banks can have quality assurance by applying security analysis based on information technology. The hackers would build awareness to the bank at all levels (Hatch et al, 2001).

Prevent security breaches

The ethical hackers can assist the bank to fight against national andterrorismsecurity breaches. In addition hiring ethical hackers could generate a computer system that hinders malicious hackers from having access to it. Moreover the hackers would ensure the banks have adequate preventive measures that are efficient in preventing security breaches. The hackers can use their skills to cause fast advancement in the banking system and this means the bank does not stagnate rather it progresses. Moreover, hackers can lead to certain innovation and diversification in the banks (Kitchen, 2010).

Disadvantagesof using hackers to test the bank security system

Hackers may turn to be malicious hackers

It is not a wonder that the ethical hackers hired by the banks to check on the security systems could turn to be malicious hackers. Applying the knowledge they gain, the ethical hackers can perform malicious hacking activities. With

this in mind it can be very dangerous for the banks to allow the hackers have to the financial as well as banking details. The hackers may develop less noble motives towards the bank and plan to steal personal information regarding the bank. At this point they may go to an extent of changing the financial date of the corporation, break the bank's security codes so as to have authorized network access and further conduct other activities that are very destructive.

There is a possibility that they may even place or send malicious viruses, codes, malware and other harmful and destructive things to the bank's computer system. In other circumstances the hackers may offer a massive security breach (Kitchen, 2010).

Hackers may gain authority in the bank system

Ethical hackers who turn to be malicious hackers will look for easy targets and look for information concerning them. Hence, they will break into the system and gain authority to control all that is involved in that system. Consequently, they will hide any evidence relating to their break-in hence complicating the prosecution process if at all they are caught. Though online banking is effective to most people, hackers can break into any computer system and therefore they pose a threat to people who happen to rely with the bank. If a hacker happens to access to an individual's bank account, it is obvious that serious irreversible damage can be created.

This would lead to lots of devastation to the individual and to the bank as well. Online casinos allow people to withdraw money using personal checks as written by the casino. Though these casinos have effective security

arrangements there is a likelihood of a hacker accessing and consequently misusing the sensitive information involved hence causing a player ruthless financial loss. These are just examples of how the hackers can affect the bank as well as individuals who benefit from the bank in terms of financial matters (Kurtz et al 1999).

4) Other alternatives for testing security system other than using hackers

Security patches

As a result of the many disadvantages associated with hackers, it is advisable for the banks to try other techniques of testing their security system rather than the hackers. It is important that the bank take advantage of the software programs that offers updates on regular basis. For instance the Microsoft provides some free security patches specifically for its internet Explorer browser.

To a certain extent the antivirus programs basically searches for fixed sections of data referred to as signatures. The antivirus stores a database of signatures for any form of virus that could have been developed by computer hackers. If it happens that the antivirus locates a signature in a certain file then it decides definitely that that file is infected with a particular virus (Polk, 2005).

Having in mind that the antivirus searches for viruses that are known, a bank will be protected from a virus or worm that exploits the browser bug if the antivirus company has already received information regarding the virus and analyzed it effectively. In addition it is required that the antivirus company had added the signature linked to the virus to the signature database. The

bank is also required to install fresh signature database in their computers. If a browser bug is not in any way exploited by some virus or worm, then the antivirus will not know about it.

Moreover, if a new version of virus or worm appears to exploit the same very bug, again the antivirus may fail to detect it. The truth of the matter is that antivirus software can save the banks a lot of trouble by at least limiting the damage that would be caused by browser bug. However, antivirus software is not known to give complete protection and hence the bank needs to look at other alternatives (Polk, 2005).

Network firewall

It is highly recommended for a bank to install a network firewall since the firewall places itself in between the internet and the organization’s networks and decides upon what data to pass through the system. Basically, network firewall formulate decision regarding the type of data to pass through and not basing on the content that is whether it contain virus or it is harmless. As a result, successful firewalls are those with content filtering capabilities or antivirus and with this the firewall will be in position to filter the data that flows to the organization’s system. This means that the firewall will detect any malicious web site that could exploits a bug in the browser and give a warning to the user.

It is advisable that the bank download and install patches that could be possibly be missing in the system. This is made possible by the Browser Security Test that offers a way of correcting the problem by providing links that directs an individual to the patch that corrects a particular problem

found in the browser. It is important that the bank keep their browser updated to prevent browser security problems (Polk, 2005).

Application security

The banks ought to understand that the law does not protect businesses from liability incase a company data is stolen and misused due to illegal infiltration. As a result, the highest priority ought to be internet security up to the moment the government comes up with a way of dealing with the perpetrators of internet fraud.

The banks should therefore consider application security which enhances standard protection for the system. In addition the penetration test recognizes where risks have entered to manual security from ‘ gaps’ (Piscitello, 2010). The tests are important because common problems that emanates from the manual security administration may leave a company vulnerable. The security gap offers entry sites for hackers to steal data.

The banks should carry out internal as well as external testing to guarantee the organization a good protection from damage and data loss. Penetrating test involves assessment of the information security measures and is usually done frequently. The findings of the assessment should then be recorded in a report which ought to be presented during a briefing session.

In the session, questions from different people in the organization can be answered and proper strategies can be discussed freely. In this test, a company may test ways in which it collects and processes data. In addition the system that stores the data, the channels of transmission, the personnel

and processes are also tested. The penetration test may be performed by an outsider who is trained in anti-hacking techniques (Piscitello, 2010).

Testing social engineering

On the other hand threats to computer crime can be assessed through testing social engineering which offers the level of trust provided to the outsiders who seek for information that they are not entitled to from the employees. Social engineering is a manner of testing whether the employees in a certain company understand the significance of restricting company security details like entry codes and log-ins. This testing may help the bank to inform employees that are not informed on the importance of keeping secrets concerning the sensitive information that if known by outsiders could result to serious computer crime (Landoll, 2006).

Bibliography

Carr, I. & Williams, K. 2005. *Computers and law* . Great Britain, Intellect Books.

Carter, D. & Katz, A. 2010. *Computer Crime: An Emerging Challenge for Law Enforcement* . [Updated on February 3, 2010] available at http://www. sgrm. com/art11. htm [Accessed July 27, 2010].

Casey, E. 2004. *Digital evidence and computer crime: forensicscience, computers and the Internet* . Great Britain, AcademicPress.

Clark, F. & Diliberto, K. 1996. *Investigating computer crime* . New York, CRC Press.

Emm, D. 2009. *Cybercrime and the law: a review of UK computer crime legislation.* [Updated on May 29, 2009] available at http://www. securelist. com/en/analysis/204792064/Cybercrime_and_the_law_a_review_of_UK_computer_crime_legislation[Accessed July 27, 2010].

Hatch, B., Lee, J., & Kurtz, G. (2001). *Hacking Linux exposed: Linux security, secrets and solutions* . Berkeley, CA : McGraw-Hill/Osbourne.

Johnson, T. 2005. *Forensic computer crime investigation* . New York, CRC Press.

Landoll, D. 2006. *The security risk assessment handbook: a complete guide for performing security risk assessments* . New York, CRC Press.

Kitchen, R. 2010. *Defining Ethical Hacking-ItsGoalsand Benefits.* [Updated on July 13, 2010] Available at http://www. brighthub. com/internet/security- privacy/articles/77412. aspx [Accessed July 27, 2010].

Kurtz, G., McClure, S., & Scambray, J. (1999) *Hacking exposed: Network security, secrets and solutions* . Berkeley, CA: McGraw-Hill/Osbourne.

Piscitello, D. 2010. *Your First Penetration Test* . [Updated on 2010] available at http://www. corecom. com/external/livesecurity/pentest. html [Accessed July 27, 2010].

Polk, W. 2005. *Automated tools for testing computer system vulnerability* . New York, DIANE Publishing.

Walden, I. (2007) *Computer Crimes and Digital Investigations,* Oxford: Oxford University Press.

Young, T. *Police fail to record e-crime* . [Updated on Nov 2, 2006] Available at http://www. computing. co. uk/computing/news/2167740/police-fail-record-crime [Accessed July 27, 2010].