**Abstract**

Information in this day and age is just a click away – this is all due to technology and digitalization of the world. For the past decade, technology has been greatly improving people’s lives in compelling ways. All is made easier from schooling to employment. In spite of the fact that the possible outcomes are just restricted by what we can think, so are the dangers for abuse of technology.

These days, businesses use technology as a tool to further improve their operation and services. Banks, in particular, have been using technology to reach out to their customers. Automated Teller Machine (ATM) is one of the technology that banks use that allow customers to withdraw money without a branch representative. In recent years, there are been a lot of cases of ATM heists, where in thieves are able to hack the ATM and withdraw money a great amount of money.

This paper will discuss the particular ATM Heist that happened in New York in 2013, along with ways to prevent the heist from happening and other related laws.

Keywords: Technology, Abuse, Automated Teller Machine, Heist, Hack.

**Introduction**

ATMs have been prime focus for criminals, incorporating both those in the physical domain and also the digital. According to a survey conducted by different banking association, there was an estimate of 3.5 million transactions of ATM crime. [6] There are various ways to steal from ATMs, Trend Micro said that thieves are using pieces of hardware that can be placed over a normal card recorder on the ATM, allowing the hacker to steal the details of the card holder who is using the machine. But Trend Micro also said that logical attacks on ATMs are gradually getting recognized, meaning that thieves are teaming up with hackers to launch attacks in the digital realm. Trend Micro discovered that the number of attacks on ATMs using malware considerably went up. It was discovered that fraud attacks on ATMs has risen up to 15% from 2014 to 2015. There were less than 7,000 (seven thousand) malware-based attacks during 2014, but it significantly rose up to more than 7,000 in 2015. [7]

In order to able to avoid such incidents, the financial institution must have regulations guaranteeing the security of the machines and it’ operating system (OS). Patching up the security of the OS will lessen the opportunity of malware infection, keeping the ATMs OS up to date is a step in the right direction. Patching up the security of the OS will lessen the opportunity of malware infection.

**Results and discussion**

Pertaining to the cybercrime which is ATM Heist, where in groups of people execute fraud and scams through the use of information that was either extracted from an account or was stolen, there are some laws to keep those crimes at bay. An example of an ATM heist being executed is an article about These laws are the ones that carries out justice to those who planned and executed this crime. One example is the $45 million (45,000,000) global ATM heist [1] In this example, they executed the withdrawal of money from ATM within the withdrawal limit. They created dummy cards that hold debit card information and loaded those dummy cards with astronomical balances [1] This resulted into large sums of money being withdrawn all over the world. This could be a problem because if they did it through the use of just dummy cards, imagine if an even larger group were to execute this kind of crime. That’s why there are laws which provides due process to those criminals.

One example is extradition laws which helps bring criminals to justice if they conducted the crime in another state or country. [2] This would help both countries, our country and the requesting country for extradition, to bring criminals with either heinous crimes or lesser crimes to proper due process according to the law. Next example is a BSP memo that enables banks to adapt to the EuroPay, MasterCard, and Visa (EMV) standard to provide a much safer transaction between ATM and other transactions as well as to prevent ATM frauds that are common nowadays [3]. This law would prevent card skimming, the illegal process of copying one’s credit card information for illegal purposes, from happening. Another law is the E-commerce Law in the Philippines or better known as R.A. No. 8792, in which it proposed a safer and better communication between electronic devices from the parties established [4] This would improve communication between devices and parties that are involved in the said communication to provide security as well as availability and convenience. As these laws protect the people from being victims of crimes and to provide justice to those who stand in the way of what is right, there are certain weaknesses and strengths that exist in the laws.

The Extradition Law, as stated earlier, is a law to help both countries bring justice to a criminal in whom which executed crimes against the law. This would help the two countries involved, the requested country and the requesting country, to properly bring the criminals to justice. The strong point of this law is that with this law, criminals who had done crimes against the law of a country and chose to fled that specific country for hiding purposes from the law, that criminal could be given back to the country where the crime happened and he/she could be given proper justice. With this law being exercised, it could lessen the unprocessed crimes or criminals not being given proper justice. But the main weakness of the extradition law is that if the criminal will face the death penalty as punishment, the requested country could deny the request of the criminal being extradited. The requested country would conduct the trial in the country and the punishment would be up to them. What if they don’t have a law in where in doing the crime of an ATM Heist is not considered a crime? That would result into the criminal going free without the right punishment. That serves as a big weakness to the law of Extradition treaties.

Next law is the BSP memo or applying EMV standard to the banks here in the Philippines. Our banks here in the Philippines still use the traditional magnet stripe (magstripe) as a way for the ATM cards to carry the specific data or key needed to access the specific account. With the problem of ATM skimming existing in the world, those with magstripe type ATM cards fall victim to such crimes. This would result into the account being hijacked and to be used with malicious intent. The strength of this law is to avoid that problem. With the EMV standard applied, obsoleting the magstripe and replacing it with a microprocessor chip that holds the data. That would completely protect the card from ATM skimming because skimming devices only work on cards with magstripe. But there is one problem that the EMV standard has and that is there are hybrid cards that are existing in the EMV standard. Hybrid meaning that these types of card have both a magstripe and the chip implanted in the card. This would make the card open to the ATM skimming crime and would get the information on the card stolen.

The last law is the E-commerce Law in the Philippines which as stated earlier, provides better communication between electronic devices. This law aims to provide the message only to the intended person and from the sender of the message. Giving privacy as well as security, this law is a good application and defense against eavesdroppers or people with the intent to listen-in to the conversation between two parties or more. With this law applied, it protects the people as well as gives the right judgment for the criminal. The strength of this law is that the given communication between the parties has security and confidentiality applied. This would limit the electronic messages to those who are intended to read the message. This is important in our society since technology is evolving every day and moves toward the digital age. Most of our communication today is done through the use of electronic devices. One problem exist however, and that problem is it only pertains to electronic messages and not to transactions in banks. Although it has a section about electronic transactions, there should be a section pertaining to the electronic transaction between ATM and the cardholder. Those entities use the ATM card as a way to communicate since it is a key and the communication between the parties should be protected and made sure that it is safe to transact. Without proper protection between the communication of the two parties, it is unsafe and prone to a third party listening.

**Conclusion and Recommendation:**

The technology nowadays seems to be more powerful compared to what it was during the past. It’s now applied in almost every activity we do. The fact the economists’ estimates that only 8% of the world’s currency exists as physical cash and the remaining percentage is stored in an server or hard drive[5], proves how powerful technology is. there are lots of technology enthusiast that knows this fact, but instead of doing good, they took advantage of what they know and use it to gather anything valuable from it, as what happened in the Twenty four million (24,000,000) ATM heist, we often referred to these people as Hackers or to be specific a black hat hacker. There were laws that were mentioned in the discussion which is used to penalize such acts referred as cybercrime.

Different institutions such as banks strictly practice security in their system, but the fact that till now, not everyone was penalize in the ATM heist, means that it prospered and there are flaws in the banking system or laws that we have right now, and they should put an effort to resolve the problem, so that I won’t happen again. Upon reviewing the flaws the researchers recommend to look at the following:

1. Negotiate or talk with other countries to have an extradition treaty. The extradition law states that if an alleged criminal has done an illegal activity on other country means that they foreign country will have the authority for trial or punishment. This would be efficient especially in cybercrimes, since it is easy to do exploits in other country by means present technology. Having this treaty would benefit both countries if a crime happened that involves the borders of authority.
2. Institutions that involves huge amount of money such as banks should monitor the network traffic in real-time. This would help in determining if there’s a remote connection that’s happening, by doing so they could detect and prevent illegal money transfer.
3. The banks should be required to follow a standardize security framework for all banking institutions before they can continue to their operations. To ensure that each and every personal information are properly secured. And if such framework exists, it should be improved and re-evaluated from time to time.

References:

[1] http://www.theverge.com/2013/5/13/4326336/cyber-caper-behind-the-scenes-of-the-45-million-atm-heist

[2] http://www.lawphil.net/statutes/presdecs/pd1977/pd\_1069\_1977.html

[3] http://www.bsp.gov.ph/regulations/regulations.asp?id=3378

[4]

http://www.wipo.int/edocs/lexdocs/laws/en/ph/ph022en.pdf

[5]

<https://www.google.com.ph/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=percentage%20of%20virtual%20money>

[6] <http://www.popcenter.org/problems/robbery_atms/>

[7] <http://blog.trendmicro.com/hackers-cash-in-on-atm-malware/>