Cybercrime & its Criminal Justice Response

Prof. Umesh Kumar Tanwar
Department of Computer Science, B.J.S. Rampuria Jain College, Bikaner-334001

Abstract: Cybercrime, also called computer crime, is any illegal activity that involves a computer or network-connected device, such as a mobile phone. The Department of Justice divides cybercrime into three categories: crimes in which the computing device is the target, for example, to gain network access; crimes in which the computer is used as a weapon, for example, to launch a denial of service (DoS) attack; and crimes in which the computer is used as an accessory to a crime, for example, using a computer to store illegally-obtained data.

Keywords: Cyber Crime, Criminal Justice

I. INTRODUCTION

The growth of the internet has enabled an increase in the volume of cybercrime activities because there is no longer a need for the criminal to be physically present when committing a crime. The internet's speed, convenience, anonymity and lack of borders makes computer-based variations of financial crimes, such as theft, money laundering or fraud, and hate crimes, such as stalking and bullying, easier to carry out.

Cybercrime may be committed by individuals or small groups, as well as by criminal organizations that are often spread around the world and committing crimes on an unprecedented scale. Cybercrime has the unusual characteristic that the victim and the perpetrator may never come into direct contact; in many cases, perpetrators and victims are separated by thousands of miles. To further reduce the chances of detection and prosecution, cybercriminals often choose to operate in countries with weak or nonexistent cybercrime laws.

II. CYBERCRIME MARKETS

“Cybersecurity is a critical issue, and as companies become more global they leave a digital footprint that can make them accessible to anyone from anywhere,” said a 2014–2015 Cushman & Wakefield report on emerging market conditions. The multinational real estate company ranked more than 40 countries on their relative risk of doing business — not just on cybersecurity — and the emerging markets of African nations such as Libya, Angola and the Democratic Republic of the Congo had the highest risk. The authors see cyberthreats on the rise, particularly as global businesses try to expand into more of the developing world.

That puts all businesses on notice. Just because these events happen in the developing world doesn’t mean they shouldn’t be monitored. To put this in perspective, cybercrime in Brazil results in over $8 billion per year in losses. The country has become the top source and destination for attacks across Central and South America.

In the U.S., we are used to thinking that because we created the internet, we have some primacy on the technology. But in the last few years, there are now more internet users in China than the U.S., and that’s translating into greater numbers of malicious actors. According to The Guardian, authorities in China recently arrested 15,000 people for alleged cybercrimes, signaling a new offensive to safeguard the internet. Police investigated more than 60,000 websites and increased efforts not only to block content, but also to insist that users register with their actual names and not pseudonyms.

There’s more: Symantec recently reported that attacks against the SWIFT financial network could be traced back to criminals in North Korea. The banking network has dominated the headlines recently with news of costly hacks around the world. This is yet another emerging cybercrime market already having a massive effect on the world.

III SECURITY WITHOUT BORDERS

Part of the problem is that many businesses in these emerging markets have limited security awareness, regulations and controls. They also don’t have the security and IT professionals needed to implement and enforce these measures.

Many Indian banks have yet to employ a chief information officer (CIO), let alone significant IT staff to operate security infrastructure or set policies. Without someone to take the lead, cloud computing security policies are practically nonexistent in the country.

In Nigeria, cybersecurity laws are barely a year old, “but many key stakeholders such as the judiciary and law enforcement agencies have yet to come up to speed in understanding and implementing” these laws, said a report from Deloitte. Nigerian IT security consultants are also in short supply, making it harder for businesses to stay on top of attacks and train their own staff properly.

We can be sure that cybercriminals are waiting in the wings to exploit growing technologies — and security-illiterate populations. Even though many of these emerging markets are just getting internet access, the best strategy is still to start with the security basics. For example, a 2015 KPMG report recommended five specific actions, including implementing basic cyber precautions such as regular software patching and
restricting data access, enforcing continuous testing for software vulnerabilities, monitoring critical systems and preparing incident response plans.

IV. CYBER CRIMES

Phishing

Phishing is a crime that involves a criminal obtaining a victim’s personal information such as their credit card or social security number. The criminal is able to acquire this information by posing as a legitimate company. They send emails or instant messages as employee of a company and ask for the victim to visit their website to input information. The victim then goes to the website. This website usually looks very legitimate and safe, and this prompts the victim to give out their information without hesitation. The criminal then uses the information they have stolen from the victim.

Online Stalking (Cyberstalking)

This cybercrime involves a victim being stalked online. The stalker will use electronic means of communication to harass and threaten the victim. They might constantly follow the victim from chatroom to chatroom or from forums. The stalker also might send the victim threatening emails frequently or harass them by social media sites. They can cause the victim fear and other problems using the computer and internet.

Credit Card Fraud

Another common cybercrime is credit card fraud. Criminals who have obtained a credit card can easily buy almost anything on the internet using it. Due to the bad security on some websites, criminals can use tools to obtain credit card numbers and information when a person purchases something online. Credit card fraud can cause major problems and can victimize several different people.

Software Piracy

A particularly damaging type of cybercrime is software piracy. This involves a criminal illegally distributing a piece of software or illegally getting a program without paying for it. By distributing the program illegally online, the criminal deprives the manufacturer and creators of the program the money they deserve.

Blackmailing

Another type of cybercrime is blackmailing. This is where a criminal will blackmail a person by threatening to post nude photographs or other materials online. In order to stop the criminal from doing it, the victim is forced to give them money or passwords to their bank account.

Cybercrimes are numerous and have victimized countless people. The internet and computers are being used to do harm, steal information, and do many different types of illegal activities. People can protect themselves from becoming victims by refusing to give information on websites that they have not verified the authenticity of. They should also only purchase items on sites that have good security.

BIBLIOGRAPHY

[13]. http://searchsecurity.techtarget.com/definition/cybercrime
[14]. https://securityintelligence.com/the-growing-threat-from-emerging-cybercrime-markets/
[15]. http://www.criminajusticedegreecub.com/what-is-cybercrime/