International Digital Organization for Scientific Research
IDOSR JOURNAL OF ARTS AND MANAGEMENT 5(1): 64-69, 2020.

Prevalence of Cyber Crime and its Effect on Economy

Mulligan, D. and Levi, M.

Department of Criminology, Faculty of Arts and Humanities, American International University West Africa, Gambia.

ABSTRACT

Governments needs reliable data on crime in order to both devise adequate policies, and allocate the correct revenues so that the measures are cost-effective, i.e., The money spent in prevention, detection, and handling of security incidents is balanced with a decrease in losses from offences. The analysis of the actual scenario of government actions in cyber security shows that the availability of multiple contrasting figures on the impact of cyber-attacks is holding back the adoption of policies for cyber space as their cost-effectiveness cannot be clearly assessed. This review article will show the impact of cyber crime on the economy.

Keywords: Prevalence, Cyber Crime, Economy Government.

INTRODUCTION

New technologies create new criminal opportunities but few new types of crime. Therefore Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy [1]. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. Because of the early and widespread adoption of computers and the Internet in the United States, most of the earliest victims and villains of cybercrime were Americans [2]. By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another.

An economy is an area of the production, distribution and trade, as well as consumption of goods and services by different agents. Understood in its broadest sense, 'The economy is defined as a social domain that emphasize the practices, discourses, and material expressions associated with the production, use, and management of resources'. Economic agents can be individuals, businesses, organizations, or governments [3]. Economic transactions occur when two groups or parties agree to the value or price of the transacted good or service, commonly expressed in a certain currency. However, monetary transactions only account for a small part of the economic domain. Economic activity is spurred by production which uses natural resources, labor and capital. It has changed over time due to technology (automation, accelerator of process, reduction of cost functions), innovation (new products, services, processes, expanding markets, diversification of markets, niche markets, increases revenue functions) such as, that which produces intellectual property and changes in industrial relations (most notably child labor being replaced in some parts of the world with universal access to education) [4]. A given economy is the result of a set of processes that involves its culture, values, education, technological evolution, history, social organization, political structure and legal systems, as well as its geography, natural resource endowment, and ecology, as main factors. These factors give context, content, and set the conditions and parameters in which an economy functions. In other words, the economic domain is a social domain of human

practices and transactions. It does not stand alone [5]. A market-based economy is one where goods and services are produced and exchanged according to demand and supply between participants (economic agents) by barter or a medium of exchange with a credit or debit value accepted within the network, such as a unit of currency. A command-based economy is one where political agents directly control what is produced and how it is sold and distributed [6]. A green economy is low-carbon, resource efficient and socially inclusive. In a green economy, growth in income and employment is driven by public and private investments that reduce carbon emissions and pollution, enhance energy and resource efficiency, and prevent the loss of biodiversity and ecosystem services.

Types of cybercrime

Cybercrime ranges across a spectrum of activities. At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or individual [7]. Also at this end of the spectrum is the growing crime of identity theft. Midway along the spectrum lie transaction-based crimes such as fraud, trafficking in child pornography, digital piracy, money laundering, and counterfeiting. These are specific crimes with specific victims, but the criminal hides in the relative anonymity provided by the Internet. Another part of this type of crime involves individuals within corporations or government bureaucracies deliberately altering data for either profit or political objectives. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet [8]. These range from spam, hacking, and denial of service attacks against specific sites to acts of cyberterrorism that is, the use of the Internet to cause public disturbances and even death.

Identity theft and invasion of privacy

Cybercrime affects both a virtual and a real body, but the effects upon each are different. This phenomenon is clearest in the case of identity theft. In the United States, for example, individuals do not have an official identity card but a Social Security number that has long served as a de facto identification number [9]. Taxes are collected on the basis of each citizen's Social Security number, and many private institutions use the number to keep track of their employees, students, and patients. Access to an individual's Social Security number affords the opportunity to gather all the documents related to that person's citizenship i.e., to steal his identity. Even stolen credit card information can be used to reconstruct an individual's identity. When criminals steal a firm's credit card records, they produce two distinct effects [10]. First, they make off with digital information about individuals that is useful in many ways. For example, they might use the credit card information to run up huge bills, forcing the credit card firms to suffer large losses, or they might sell the information to others who can use it in a similar fashion. Second, they might use individual credit card names and numbers to create new identities for other criminals. For example, a criminal might contact the issuing bank of a stolen credit card and change the mailing address on the account. Next, the criminal may get a passport or driver's license with his own picture but with the victim's name [11]. With a driver's license, the criminal can easily acquire a new Social Security card; it is then possible to open bank accounts and receive loans all with the victim's credit record and background. The original cardholder might remain unaware of this until the debt is so great that the bank contacts the account holder. Only then does the identity theft become visible. Although identity theft takes places in many countries, researchers and law-enforcement officials are plagued by a lack of information and statistics about the crime worldwide. Cybercrime is clearly, however, an international problem [12].

Wire fraud

The international nature of cybercrime is particularly evident with wire fraud. One

of the largest and best-organized wire fraud schemes was orchestrated by Vladimir Levin, a Russian programmer with a computer software firm in St. Petersburg. In 1994, with the aid of dozens of confederates, Levin began transferring some $10 million from subsidiaries of Citibank, N.A., in Argentina and Indonesia to bank accounts in San Francisco, Tel Aviv, Amsterdam, Germany, and Finland [13]. According to Citibank, all but $400,000 was eventually recovered as Levin's accomplices attempted to withdraw the funds. Levin himself was arrested in 1995 while in transit through London's Heathrow Airport (at the time, Russia had no extradition treaty for cybercrime). In 1998 Levin was finally extradited to the United States, where he was sentenced to three years in jail and ordered to reimburse Citibank $240,015. Exactly how Levin obtained the necessary account names and passwords has never been disclosed, but no Citibank employee has ever been charged in connection with the case. Because a sense of security and privacy are paramount to financial institutions, the exact extent of wire fraud is difficult to ascertain [14]. In the early 21st century, wire fraud remained a worldwide problem.

Impacts of Cyber-Crime

Lunda Wright, a legal researcher specializing in digital forensic law at Rhodes University, has an interesting research finding on a blog posted in October 2005. It states that there has been an increased rate of prosecutions of cyber-criminals. There has been an increased clamping down on cyber-piracy related to the film and music works. There are novel lawsuits and strategies for litigation. There is a greater dependence on the skills of computer forensic experts in corporations and government. Finally, there is an increase in inter-government cooperative efforts. Organized crime groups are using the Internet for major fraud and theft activities. There are trends indicating organized crime involvement in white-collar crime [15]. As criminals move away from traditional methods, internet-based crime is becoming more prevalent. Internet-based stock fraud has earned criminals millions per year eading to loss to investors, making it a lucrative area for such crime. Police departments across the nation validate that they have received an increasing number of such crimes reported in recent years. This is in sync with the national trend resulting from increased computer use, online business, and geeky sophisticated criminals. In the year 2004, cyber-crime generated a higher payback than drug trafficking, and it is set to grow further as the use of technology expands in developing countries. Scott Borg, director of the U.S [15]. Cyber Consequences Unit, an agency supported by the U.S. Department of Homeland Security, recently indicated that denial-of-service attacks won't be the new wave of future. The worms, viruses are considered not quite mature as compared to the potential of attacks in future.

1. Potential Economic Impact

The2011 Norton Cyber crime disclosed that over 74 million people in the United States were victims of cyber crime in 2010 [16]. These criminal acts resulted in $32 billion in direct financial losses. Further analysis of this growing problem found that 69 percent of adults that are online have been victims of cyber crime resulting in 1 million cyber crime victims a day. Many people have the attitude that cyber crime is a fact of doing business online. As today's consumer has become increasingly dependent on computers, networks, and the information these are used to store and preserve, the risk of being subjected to cyber-crime is high. Some of the surveys conducted in the past have indicated as many as 80% of the company's surveyed acknowledged financial losses due to computer breaches [17]. The approximate number impacted was $450 million. Almost10% reported financial fraud. Each week we hear of new attacks on the confidentiality, integrity, and availability of computer systems. This could range from the theft of personally identifiable information to denial of service attacks [12]. As the economy increases its reliance on the

internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy. The disruption of international financial markets could be one of the big impacts and remains a serious concern [13]. The modern economy spans multiple countries and time zones. Such interdependence of the world's economic system means that a disruption in one region of the world will have ripple effects in other regions. Hence any disruption of these systems would send shock waves outside of the market which is the source of the problem. Productivity is also at risk attacks from worms, viruses, etc take productive time away from the user. Machines could perform more slowly; servers might be in accessible, networks might be jammed, and so on. Such instances of attacks affect the overall productivity of the user and the organization. It has customer service impacts as well, where the external customer sees it as a negative aspect of the organization [9].

2. Cyber-Attacks on Stock Prices

Thus far, reported cyber-attacks have been relatively limited in scope, and have not yet been on a scale that would have significant macroeconomic consequences. Individual firms, however, may have suffered significant losses as a result of past attacks. An examination of the effects of those attacks might be illuminating [4]. Most estimates of the cost to companies of cyber-attacks are based on surveys. Survey responses are often expressed in such a wide range as to indicate considerable subjectivity and thus they may be of limited use. There may, however, be a more objective measure of the effect of cyber-attacks on individual firms [7]. In theory, the price of a company's stock is primarily determined by the present discounted value of the cash flows expected to result from that firm's output. That cash flow is what contributes to the wealth of the stockholders, either in the form of dividends or in the expansion of the firm's stock of productive capital. Any event that changes investors' expectations about that future stream of income is likely to affect the price of the stock. Four recent studies have examined a number of actual cyber-attacks in an effort to see if any of those attacks could be linked to a change in the stock prices of the affected companies. In some cases, the studies attempted to measure if any stock-price effect depended on the different characteristics of either the firm or the attacks [10]. It seems at least intuitively obvious that some firms are more exposed to cyber-attacks than are others. It is conceivable that firm size may affect vulnerability to attack, but more to the point some firms are more dependent on computer networks than others to conduct business. Conventional firms, which have been referred to in this context as "brick and mortar" firms, might be expected to be the least vulnerable to cyber-attacks as they are the least dependent on the Internet to conduct business [7]. Some firms, characterized as "click and mortar," conduct business both off-line and over the Internet. These firms face an increased vulnerability because of the risk that the business they conduct via the Internet might be interrupted. Finally, there are firms whose business is conducted almost exclusively over the Internet. These firms would seem to be most at risk. The extent to which a business is affected might reasonably be expected to depend on the type of attack. Most attacks have fallen into one of two categories [2]. The first is a "denial-of-service" attack (DoS). A DoS attack renders a firm's Internet portal inaccessible and interferes with its ability to conduct on-line business. For the most part, this kind of attack causes no lasting harm. The more serious category of attacks are those that involve the theft or destruction of secure information. This kind of security breach is more likely to have lasting effects on the targeted firm. Other things being equal, the more dependent a firm is

on the Internet, and the more intrusive an attack is, the more likely it is that any attack will have significant consequences for the financial health of that firm [1].

3. Impact on Consumer trust

Since cyber-attackers intrude into others'space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long term basis. The site in question is termed as the fraudulent, while the criminal masterminding the hidden attack is not recognized as the root cause [13]. This makes the customer lose confidence in the said site and in the internet and its strengths. According to reports sponsored by the Better Business Bureau Online, over 80% of online shoppers cited security as a primary worry when conducting business over the Internet. About 75% of online shoppers terminate an online transaction when asked for the credit card information [8]. The perception that the Internet is rife with credit card fraud and security hazards is growing. This has been a serious problem for e-commerce. Complicating the matter, consumer perceptions of fraud assess the state to be worse than it actually is. Consumer perception can be just as powerful or damaging as fact. Hence users'concerns over fraud prevent many online shoppers from transacting business. Concern over the credibility of an e-business in terms of being unsafe or cluttered makes a shopper reluctant to transact business [12]. Even the slightest perception of security risk or amateurish commerce seriously jeopardizes potential business.

CONCLUSION

It might be expected in a study of the effects of past attacks that a pure Internet company whose network security is breached would suffer more than would a conventional firm that is affected by a DoS attack. But, it might also be presumed that those firms are fully aware of their respective vulnerabilities and so they allocate resources to computer security to differing degrees. In contrast, firms that provide computer security might be expected to benefit from cyber-attacks (unless their products were publicly blamed for an attack's success). An increase in the apparent vulnerability of computer networks could be expected to raise future earnings of those companies and thus boost their stock price. This also could help cope with the economic breach caused by cyber crime.

REFERENCES

1. Anderson, R. and Moore, T. (2017). The economics of information security. Science, 314(5799):610—613.
2. Becker, G. (2019). Crime and punishment: An economic approach. *The Journal of Political Economy*, 76(2):169—217.
3. Camp, L. (2011). Re-conceptualizing the role of security user. *Daedalus*, 140(4):93—107.
4. Denning, D. (2015). Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. Networks and netwars: The future of terror, crime, and militancy, pages 239--288.
5. Ehrlich, I. (2018). Crime, punishment, and the market for offenses?, *Journal of Economic Perspectives,* 10(1), pp 43–67.
6. Finklea, K. M. and Theohry, C. A. (2012). Cybercrime: Conceptual issues for congress and U.S. law enforcement. Technical report, Congressional Research Service.
7. Gözenoglu, M., Morawe, R. (2011). The German Anti-Botnet Advisory Center. Presentation at 'Internet Security Days', 13–15.
8. Kshetri, N. and Dholakia, N. (2012). 'Determinants of the global diffusion of B2B E-commerce', *Electronic Markets*, 12(2): 120–129.
9. Levi, M. (2011). Social reactions to white-collar crimes and their relationship to economic crises. In:

Deflem, M. (ed.) Economic Crisis and Crime, pp. 87–105. The JAI Press/Emerald, London/Bingley.
10. Levi, M. and Burrows, J. (2015). Measuring the impact of fraud in the UK: a conceptual and empirical journey. *Br. J. Criminol.* 48, 293–318.
11. Moore, T. and Clayton, R. (2007). Examining the impact of website take-down on phishing. In: Cranor, L.F. (ed.) Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit, Pittsburgh, vol. 269, pp. 1–13, 4–5.
12. Mulligan, D. and Schneider, F. (2011). Doctrine for cybersecurity. Daedalus, 140(4):70—92.
13. Snow, G. (2011). Cyber security: threats to the financial sector. Testimony before the House Financial Services Committee. http://financialservices.house.gov/UploadedFiles/091411snow.pdf
14. Yar, M. (2019). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal of Criminal Justice*, 44(4):387—399.
15. Moore, T., Clayton, R. and Anderson, R. (2019). The economics of online crime, *The Journal of Economic Perspectives*, vol. 23, no. 3, pp. 3-20.
16. Huey, L., Nhan, J. and Broll, R. (2013). Uppity civilians and cybervigilantes: The role of the general public in policing cybercrime, *Criminology and Criminal Justice*, vol. 13, no. 1, pp. 81-97.