Good cybercrime: trends and future essay example

Sociology, Social Issues

Cybercrime: Running and operating

Introduction

In discussing cybercrime, President Barack Obama stated that cyber criminals stole as much as one trillion dollars from companies and businesses across the world in 2013. The foreboding threat of cyber-criminality and the relative ease of accessing databases across the globe, countries and companies are faced with the enormous challenge of not only countering the problem, but also innovating their operations and cyber infrastructure.

Crimes committed with the use of cyber-technology are common crimes, the difference being these crimes are amplified by the “ use of computers, computer networks, and other forms of information technology.” Compared to cyber dependent acts of criminality, these can be done without the use of ICT (McGuire Dowling, 2013, p. 1).

What types of scams are associated with the cybercrime?

Cyber-data theft is one of the more popular forms of fraud done online. Cyber criminals can send fraudulent messages by asking the targets for their identification information and other personal data. “ Spear phishers”-criminals that target specific sectors in the hope that they can net some victims-send electronic mail message asking their potential targets to log in to the “ company website” and provide their personal and financial information in order to resolve a fictitious problem with their orders.

With the fact that majority of these transactions are done online without any personal contact, guaranteeing the legitimacy of the identity of the “

company representative” has become a major consideration in the safety of the consumers in the market. With this in mind, the forgery and misappropriation of “ identity-related theft has become as established as the existence of fraud itself; terms such as “ identity theft” have been used almost synonymously with the crime of fraud and this imbrications have been critical in the develop of the vagueness in the understanding of the terms.

McGuire and Dowling (2013) proffer that in terms of online financial losses; the number of people who have experienced this instance remained low in comparison to other adverse impacts related to online usage. However, in terms of identity fraud, there is an issue in terms of the public disclosing and understanding accurately the parameters of the crime (McGuire and Dowling, 2013, p. 4).

Paragraph 1030 (a) (4) criminalizes acts of fraud against “ protected computers” or computers that have an impact to interstate and overseas trade, those in use by the Federal government, of those utilized by and for a financial organization. However, there is some degree of vagueness whether the phrase “ United States government” can also include computers being utilized by Congress and the judicial branches of government or those being used by autonomous government branches (Doyle, 2010, p. 46).

What might the profile be for a cybercriminal who commits this type of cybercrime?

Many analysts find a resilient trend associated to the corporate factors of cybercrime. The corporate inclination of the cybercrime activity includes a business archetype, corporate plans, and even pricing structures copied from

the business world and the customer service business models. This fact establishes the fact that the common stereotype of an “ independent hacker” in the cybercrime world will soon be irrelevant and be replaced with a “ professional force” hired to execute a specific task based on the skills of the team members. These teams will work in shifts to distribute the task as well as the liabilities owing to the global nature of the crime.

This shows that the specifications of the teams or the members of the teams are nationality oriented. There are groups from different countries; for example, groups from China will supply the software needed for the commission of the crime, and a Japanese group will be the ones handling the hardware. In addition, there will be specialized groups that will solely focus on the aspects of propaganda, undermine the corporate structure, and deception by using social networks and then utilize methods and practices that have traditionally been associated with counterfeiters.

These mercenary groups sell their services to the highest bidder. It does not manner whether the group that “ acquired” their services will be an extremist organization, large industrial concerns, or hostile nations that utilize advanced “ off-the-shelf” tools and technology to attack the target’s system, deception and propaganda, which these groups can use in order to attain their financial or political objectives. Aside from hired cybercriminals, many observers believe that hostile nations will turn a portion of their defensive arsenal and offensive weaponry to restore order a modicum of deterrence in cyberspace.

However, it would be difficult to ascertain a specific profile to be assigned to a cybercriminal. The dilemma is due to the growing spread of technology, “

employers” who have conflicting interests, and that the base of suspects is one that no one stands out. Terrorists and other fundamentalist groups are difficult to trace owing to the use of the “ multiplier effect” of the media in being able to disseminate their agendas (McAfee, 2011, p. 26). What are law enforcement initiatives to combat this crime?

The “ corporatization” of fraud has resulted in an increase in large scale data leaks as well as an increase in the frequency and magnitude of high volume fraud assaults (Britton, Katz, Gross, 2014, p. 12). Other laws that are designed to counter other crimes have been used in combination with cybercrime laws in order to prosecute these criminal elements. The Hobbs Act, 18 U. S. C. 1951, bans extortion activities that will have an adverse impact on trade and commerce. Anyone who “ obstructs, delays, or affects commerce or the movement of any article or commodity in commerce by extortion or attempts or conspires so to do shall be fines under this title or imprisoned not more than twenty years, or both.”

However, the problem here is the narrow construction of the term “ property.” The concern of Congress in that the action can be thwarted by a too constricted interpretation of the term; the dilemma lies in the apprehension that a computer system, or the data stored on the computer on computer disks, may be construed as too ethereal to be able to avail of the legal safeguards that is available to more “ real” pieces of property. In this light, the concern of Congress is that the protections given to more tangible property may not be given, either in part or in total, to pieces of property that cannot be physically held or appreciated with the senses (Doyle, 2010, p. 66).

What are penalties for committing these crimes?

Infringements are culpable by prison sentences of “ not more than 5 years, 10 years for consecutive violations, and a fine of not more than $250, 000 for individuals and not more than $500, 000 for companies. This sentencing policy is the same for the crime of fraud as stated under paragraph 1030 (a) (4) and for damages under paragraph (a) (5). The increase in the penalties is founded on the amount of the loss and damage done, and these are likely to be more widespread in the context of the release of a “ worm” or a “ virus (Doyle, 2010, p. 64). Conclusion

There is a debate on whether the appropriate policy and measures in dealing with cybercrime should be legislative or executive in origin. In essence, the problem is that the judiciary, legislative and the executive branches are exchanging calls for policies and programs that will help in effectively tackling cybercrime, and its elements, and removing it as a threat to individuals and companies. In addition, given the global nature of cybercrime and the international identity of cybercriminals, there must be a general consensus on the policies that will be universally adopted, and implemented, to be able to counter the threat of cybercrime.

Nevertheless, education remains the best weapon in the eradication of cybercrime, be it the “ simple” spamming and data phishing to the more damaging theft of corporate and national information stores. It is only when there is a general agreement can the threat be completely eradicated.

References

Britton, D., Katz, E., Gross, M. (2014). “ The growing threats of cybercrime.” Retrieved 21 June 2014 from < http://www. the41st.

com/sites/default/files/41st-Parameter-Cyber-Crime-Whitepaper. pdf>

Doyle, C. (2010). “ Cybercrime: an overview of the Federal Computer Fraud and Abuse Statute and related Federal criminal laws.” Retrieved 21 June 2014 from < http://fas. org/sgp/crs/misc/97-1025. pdf>

EMC (2014) “ Knowledge sharing and exploration workshops helping organizations in identifying, preventing and countering cybercrime.” Retrieved 21 June 2014 from

EMC (2014). “ The current state of cybercrime 2013: an inside look at the changing threat landscape.” Retrieved 21 June 2014 from < http://www. emc. com/collateral/fraud-report/current-state-cybercrime-2013. pdf>

McAfee (2011). “ Prospective analysis on trends in cybercrime from 2011 to 2020.” Retrieved 21 June 2014 from < http://www. mcafee. com/nl/resources/white-papers/wp-trends-in-cybercrime-2011-2020. pdf>

McGuire, M., Dowling, S. (2013). “ Cyber crime: a review of the evidence.” Retrieved 21 June 2014 from