

Cybercrime

by D Denys

Submission date: 28-Nov-2018 05:07 PM (UTC+0500)

Submission ID: 1046330313

File name: Policing_Cyberime.docx (25.57K)

Word count: 2598

Character count: 13817

Running head: A Book Review on Policing Cybercrime

A Book Review on Policing Cybercrime

[Name]

[Institution Affiliation]

[Course]

[Date]

INTRODUCTION

As the world transforms into the digital era every day making almost every part of our lives almost one hundred percent dependent on technology, cybercrime remains to be an issue of concern. Technology is experiencing adverse challenges irrespective of how it seems to solve almost every problem in the world. Cybercrime translates to activities done via the computer with the ill motive of hurting other people or organizations or damaging their reputations. Some of these activities include copyright infringements, inappropriate sexual content, hacking and frauds. Cybercrime becomes more difficult to deal with when the policing is not effective, (Wall & Williams 2013).

REVIEW

Peter Gottschalk in his book attempts to address the issue of policing of cybercrime. I find this book interesting in that the author focuses on all angles that could define cybercrime. Most people understand cybercrime in a shallow aspect based on the usual online crimes we encounter daily such as threats and humiliations online. Gottschalk takes interest to take the reader deeper on almost everything that could define cybercrime. Chapter one of his book describes cybercrime on different grounds ranging from computer crime on the internet, financial computer crime to white collar crimes. His explanation into the business perspective gives a wider understanding of our obvious.

He points out that an attack could be made online against a business with the aim of acquiring their proprietary information and using it for some malicious purpose or even selling it. In such a situation, I always thought that cybercrime is mostly committed by attackers from the outside of an organization. Gottschalk points out that it is actually mostly committed by attackers

within the walls of the organization. However, I find his explanation not quite fully satisfactory and sensible to say that most of the business cybercrimes come from the inside considering the nature of attacks from the outside and those from the inside. Those from the inside are nothing to compare to those from the outside. This is because his explanations of those that occur from the inside seem to be minor and petty. He includes activities such as following up on sporting events and gambling online while at work. Following a sporting event is petty; your boss is not even likely to know that you are doing so.

The effect it could have on the performance of the company is also not as serious as the one from an outsider who accesses a company's confidential information. Perhaps the employee could remain less productive, which could be fixed with simple organizational policing on the use of the internet unlike such an attack from the outside which could even cost the company its existence. The author gives more detail to the nature of cybercrime when he cuts through a white-collar attack either from the angle of the offender or the offended. This makes more sense when he points out that the less privileged in the society are not the only ones committing cyber-crime. The rich also do so. The difference is in the type of crime since the high class would be committing high-class crimes such as money laundering unlike the less privileged who are usually conning people online, (Marc 2013).

Another very significant bit that the author has handed is a financial crime. This is a very sensitive almost every individual or organization is vulnerable to if they do not have strong cybersecurity measures. Gottschalk categorizes financial theft into four categories. Fraud, theft, manipulation, and corruption. He categorizes fraudulent activities as those involving banks, checks, credit cards, and embezzlement. Theft involves cash, art, and inventory. Manipulation involves bankruptcy, laundering, and extortion while corruption involves activities such as

bribery and kickbacks. I find this breakdown easy and detailed enough for any reader to understand the author's content on this topic since most people perceive cybercrime as general as it sounds unaware of the specific categories. The author also gives a highlight of various cases of cybercrime. These range from money laundering, bank fraud, advance fee fraud, malicious agents, stock robot manipulation, identity theft to digital piracy. The author is keen to lay out the fact that cybercrime is a global challenge.

In all these cyber-crime cases, all of them happen in different geographical regions. Fake websites are a common thing in the United States, although some are done by attackers from the outside linking attempting to link them to online money channels such as PayPal and American Express. The author points out sources of illegal money that would definitely require one to launder money such as drug trafficking, robbery and winning casino games. These are activities that would happen almost in every country. Advance fee fraud has been quite rampant in Nigeria and other cases of robot manipulation in Norway to tamper with the stock exchange (Beek 2016). The author's diversification of cybercrime attempts to make it clear how much cybercrime is a global concern.

The author also explains another type of cybercrime; intellectual property crime. He explains how much this is a concern to manufacturing industries due to the making of imitated products. Worse is how easy it is to do so since it's not as complex as getting into a museum and grabbing an art to go make a copy of it. Here, the thief only needs to make an electronic copy of the product and then the actual manufacturing is done. The author touches on some industries that are quite vulnerable to it such as a car, pharmaceuticals, and filmmaking companies. This section of this book attempts to show how much technology is a necessary evil.

Child grooming is another very sensitive area of cybercrime. Gottschalk breaks the category of offenders into two, those that use minors to upload illegal sexual content on the internet and those that download such content. He states that the European Union confirms that advancement in information **technology** information technology has made such abuse of children quite possible and easy to commit. His statement actually makes more sense now that it is quite easy to commit these crimes and earn reasonable profits with very minimal risks. The author, states that viewing inappropriate child images in **the** United and Norway is an offense.

The provision of the legislation of the EU on this issue makes it a crime in all member states. The author states that some countries, however, choose to ignore the law due to their already existing **legislation** especially since their age of consent does not allow the recommended laws on the matter. The author's point here is that formulating legislation to curb child grooming and the decision to adhere to it more or less remains in the hands of each individual country. Which makes more sense why it is still difficult when enforced at an individual country's level unlike at a more universal level like through a body like the EU.

Although the book tackles many significant features of cybercrime, I would say **my the** main area of interest and what should be for any cyber policing agents and the government is in chapter four. **This particular chapter attempts to handle the ways in which cybercrime is technically handled by law enforcement agencies and governments.** It is already happening and technology remains to be a double-edged sword, (Marc 2013). It brings about new and better ways of doing things and at the same time gives more opportunities for committing cyber-crimes. I tend to think that this chapter tackles the weighty bit of the entire book. It provides a broader overview of what characteristics would define a cyber-criminal and how they can be easily identified by running the reader through a general criminal profiling tool.

I might want to think that only criminal law enforcement officers would understand the nature of a **cybercriminal** from viewing their profile. Therefore, Gottschalk does the reader better by providing such a tool that an ordinary person could not probably interpret. He does not just dive in to give us solutions to **cybercrime** but rather provides another part of the policing that I find very significant. The characteristics of the offender in a profile include sex, age, marital status, **work ethic**, skills, and medical history. He highlights the pattern in an age that would explain the nature of the criminal. He points out that **if the crime was for less than a hundred thousand dollars, the** offender could range between twenty to twenty-five years, either sex and still low on the organizational corporate ladder. An offense involving more money would mean a much older person. The cause would be dictated by greed for money rather than hate and revenge.

The author further explains some two theories that provide insights into how white collar criminals deny their crimes. He now brings us into the real world and how self-defense from potential cybercrime offenders revolves about. This is pretty much what happens in **real life** situation. The theory of neutralization theory to me makes complete sense. They use five techniques; one is denying responsibility where the criminal justifies that the act of crime was beyond his control. **Two, denial of injury.** The criminal rationalizes the crime by minimizing the harm associated with **it** especially claiming that an attack via a computer does not harm people. Three is a defense of necessity. That the situation left the criminal no choice, for instance **when** dealing with tight deadlines. Four is condemning of **condemners**. Crime is committed and blamed on targets or law for being unreasonable. Five, appealing to higher loyalties. This is when there is a dilemma and can only be fixed by committing a crime.

He also touches on the deterrence theory that points out that potential criminals can feel the fear of committing a crime and facing the punishments put in place. They tend to think keenly before committing a crime. This theory is also quite practical since normally criminals would commit a crime where the chances of getting away with it are high given that there are punishments for the crime. The two theories quite make sense. However, the author only uses them to refer to the crimes against an organization. He does not relate them to an individual against whom cybercrime has been committed. The pattern the criminal profile uses only describes the setting of an offender in the organization. What about the crimes against an individual such as child grooming? Would those characteristics define the possible cause of the crime as they do for a crime involving more money in an organization setting?

His overview of the policing in this chapter is quite diverse; he analyzes the legislation on cybercrime in the United States, Norway and also tackles some issues on financial cases in China. I admire this kind of diversification since it continues to emphasize the global nature of cybercrime. Gottschalk also addresses the issue of cyberspace. Curbing cybercrime has been challenged by a lack of awareness of the cyberspace of different geographical regions. Questions are raised every day concerning cyberspace, for instance, if a person committed a cyber-crime in a country where there is no legislation on cyberspace and they are arrested in the united states, are they supposed to be prosecuted and on what legislative terms, (Denning & Georgetown univ 2014).

The issue even becomes more complex even when handled to the police. For instance, in the case of stealing money, it is already transferred to accounts in other countries, fake websites and emails hosted in other countries. The author, therefore, shows us the significance of having well-defined cyberspace boundaries if at all the world has to succeed in curbing cybercrime.

In addressing cybersecurity, the author explains the provisions and regulatory power of the Islam faith under the Sharia law. The law is believed to preserve property, intellect, life, religion, and honor, (Marissa 2016). In as much as Muslims observe the Sharia law, in my view, it still would not be quite helpful in addressing cybercrime. Some Muslims still commit cyber-crimes under the Islam umbrella to facilitate terror attacks. Sharia is therefore just a tip of the iceberg; more viable legislation makes it effective.

Gottschalks' analysis of policing of cybercrime extends to how it relates to corporate reputation. He highlights the resource-based theory that explains that corporate reputation is a resource that could be retained to the good of a company or could lead to permanent damage. He also takes the reader through the determinants of a corporate reputation. I find his explanation quite reflective and systematic because he first poses the question on the factors considered in making a judgment on an organization. This gives the reader a moment to think critically. He then explains other factors apart from white collar crimes that include substantive and symbolic attributes. His research also finds employee motivation and competencies a factor.

Like I mentioned earlier, his approach is quite systematic. He explains the corporate reputation, its determinant factors as well as how much of an asset or liability it can be. He then proceeds to the impacts cybercrime has on it and further expounds on how to rebuild a damaged one. These way organizations can find their way out of this mess. The book also provides highlights on the business intelligence. The author points out that it is important for businesses to implement intelligence strategies. These will help them detect and predict cyber-crimes and ensure safe storage of data and confidential company information.

To emphasize how viable business intelligence is, the author gives an example of intelligence-led policing conducted in West Surrey in the United Kingdom. The intelligence was to analyze vehicle crimes and provided specifics such as where the vehicle was dumped when it was stolen, what was in it at the time and locations of the event. It was then reported to the police. I, therefore, would agree with the author that business intelligence is required in attempting to curb cybercrime.

He also covers investigations of cybercrime. The author explains the nature of a detective in a crime. I find it interesting since most of us are usually victims in case the crime occurs. Rarely shall we ever find ourselves in the detective's shoes? We only report, respond to questions and leave them to do the rest. So understanding both sides of the scenario is quite interesting. The author explains the characteristics of detectives as open-minded, curious, critical thinkers and has adequate legal knowledge.

CONCLUSION

Article Error (ETS)

The author takes keenly takes us through the aspect of policing cybercrime. I find his book easy to understand and a significant guide to policing of cybercrime. Its packaging deserves an ovation. It is one that every stakeholder in policing of cybercrime should read. It is also an important book for students and lawyers dealing with such cases as a reference. However, the book only seems to be available on Bookboon.com only. The book should be easily found and on multiple online stores for ease of accessibility for any interested reader.

REFERENCES

- Beek, J. (January 01, ²2016). Cybercrime, police work, and storytelling in West Africa. *Africa: Journal of the International African Institute*, 86, 2,
- Denning, D. E., Baugh, J. W. E., & Georgetown Univ Washington Dc. (2014). *Hiding crimes in the Cyberspace* (PREPRINT). United States:
- Marissa, M. (July 01, ⁵2016). Policing cybercrime and cyber terror. *Security Journal*, 29, 3.)
- ⁴Wall, D. S., & Williams M. L. (December 01, 2013). Policing cybercrime: *networked and social media technologies and the challenges for*
- Marc, G. (January 01, 2013). ³Crime and policing in virtual worlds: On the ever-evolving nature of cybercrime. *Freedom from fear*, 2013, 7, 52-65.

Cybercrime

ORIGINALITY REPORT

4%

SIMILARITY INDEX

3%

INTERNET SOURCES

1%

PUBLICATIONS

3%

STUDENT PAPERS

PRIMARY SOURCES

1

www.slideshare.net

Internet Source

2%

2

Submitted to Cardiff University

Student Paper

1%

3

www.pulj.org

Internet Source

1%

4

Submitted to Macquarie University

Student Paper

1%

5

Submitted to University of Wales Swansea

Student Paper

<1%

Exclude quotes

Off

Exclude matches

Off

Exclude bibliography

Off

Cybercrime

PAGE 1

PAGE 2



Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.



P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 3



P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.



Prep. You may be using the wrong preposition.



S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.



Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 4



Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.



P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 5



Missing "," You may need to place a comma after this word.



Article Error You may need to remove this article.



Missing "," You may need to place a comma after this word.



Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.



P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 6



Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.



Missing "," You may need to place a comma after this word.



Article Error You may need to remove this article.



Article Error You may need to use an article before this word.



Article Error You may need to use an article before this word.



Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sent to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.



Missing "," You may need to place a comma after this word.



Missing "," You may need to place a comma after this word.



Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.

PAGE 7



Article Error You may need to remove this article.



Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sent to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.



P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.



Prep. You may be using the wrong preposition.



Missing "," You may need to place a comma after this word.



Missing "," You may need to place a comma after this word.



Sp. This word is misspelled. Use a dictionary or spellchecker when you proofread your work.



Article Error You may need to remove this article.



Possessive You may need to use an apostrophe to show possession.



Article Error You may need to use an article before this word.