Osgoode Hall Law Journal

Volume 56 | Issue 3 Article 7

12-16-2020

Industry of Anonymity: Inside the Business of Cybercrime, by Jonathan Lusthaus

Robert Van de Mark
Osgoode Hall Law School of York University

Book Review

Industry of Anonymity: Inside the Business of Cybercrime, by Jonathan Lusthaus

Abstract

In Industry of Anonymity: Inside the Business of Cybercrime, Jonathan Lusthaus attempts to demystify the increasingly sophisticated business of cybercrime and examine how it has matured into a large, profit-driven industry. Through interviews with hundreds of subjects involved in the cybercrime industry in varying capacities, Lusthaus has sought to draw a map that, by showing how seemingly disparate elements in the industry relate to one another, can better explain how the cybercrime industry functions. In particular, Lusthaus strives to produce a better understanding of the people behind cybercrime and the contexts in which they operate. By doing so, the book endeavors to lift the veil of anonymity that has historically hidden cybercrime offenders and their activities from public view.

Book Review

Industry of Anonymity: Inside the Business of Cybercrime, by Jonathan Lusthaus[1]

ROBERT VAN DE MARK[2]

In *Industry of Anonymity: Inside the Business of Cybercrime*, Jonathan Lusthaus attempts to demystify the increasingly sophisticated business of cybercrime and examine how it has matured into a large, profit-driven industry. Through interviews with hundreds of subjects involved in the cybercrime industry in varying capacities, Lusthaus has sought to draw a map that, by showing how seemingly disparate elements in the industry relate to one another, can better explain how the cybercrime industry functions. In particular, Lusthaus strives to produce a better understanding of the people behind cybercrime and the contexts in which they operate. By doing so, the book endeavors to lift the veil of anonymity that has historically hidden cybercrime offenders and their activities from public view.

CYBERCRIME HAS BECOME AN increasingly alarming threat on a global scale. A number of recent high-profile data breaches have demonstrated the devastating impact that cybercriminals can have on both businesses and consumers. In 2013, Yahoo's email service was hacked. The breach affected up to three billion accounts and became known as the largest corporate data security breach of all time.[3] Only a few years later, a worldwide cyberattack targeted computers by encrypting data and demanding ransom payments from users in return for a key to unlock

1. (Harvard University Press, 2018).
2. JD/MBA (2019), Osgoode Hall Law School and the Schulich School of Business, Toronto, Canada.
3. Renae Reints, "Yahoo Agrees to $50 Million Settlement for Those Affected by the 2013 Data Breach" (24 October 2018), online: *Fortune Tech* <www.fortune.com/2018/10/24/yahoo-settlement-data-breach> [perma.cc/PDS2-T3F5].

their devices. This attack, caused by a malicious software called the WannaCry ransomware cryptoworm, infected over 300,000 computers across 150 nations and led to billions of dollars in losses.[4] Perhaps the most notable breach in recent years involved the American consumer credit-reporting agency Equifax, which revealed that illegitimate access to its credit-report databases had led to the breach of personally identifiable information for over 148 million people in 2017.[5] The data obtained by hackers included immutable information, such as Social Security numbers and dates of birth, effectively exposing victims of the breach to an increased risk of identity theft for the rest of their lives. These incidents and many others highlight the troubling, high-stakes nature of profit-driven cybercrime.

One recent study has estimated that global losses from cybercrime amount to close to 600 billion USD yearly and are continually growing.[6] Despite the significant losses and greater public attention to the subject, the phenomenon of cybercrime remains foreign to most people. Since attacks occur through cyberspace and are orchestrated by unseen and unknown actors, there is a certain "mystification" of cybercrime and the humans behind it.[7]

In *Industry of Anonymity: Inside the Business of Cybercrime*, Jonathan Lusthaus attempts to demystify the increasingly sophisticated business of cybercrime and examine how it has matured into a large, profit-driven industry. Through interviews with hundreds of subjects involved in the cybercrime industry in varying capacities, Lusthaus has sought "to draw a map that, by showing how seemingly disparate elements [in the industry] relate to one another, can better explain how the cybercrime industry functions."[8] In particular, Lusthaus strives to provide a better understanding of the people behind cybercrimes and the contexts in which they operate. By doing so, the book endeavors to "lift the veil of anonymity that has [historically] hidden cybercrime offenders and their activities from [public] view."[9]

---

4. "Cyber-attack: US and UK blame North Korea for WannaCry" (19 December 2017), online: *BBC* <www.bbc.com/news/world-us-canada-42407488> [perma.cc/T8G6-S3C4] [*BBC*].
5. See Glenn Fleishman, "Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes, New Report Says" (7 September 2018), online: *Fortune Finance* <www.fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary> [perma.cc/3RK6-JSK4].
6. See James Lewis, "Economic Impact of Cybercrime—No Slowing Down" (February 2018) at 4, online (pdf): *Center for Strategic and International Studies* <www.csis.org/analysis/economic-impact-cybercrime>.
7. Lusthaus, *supra* note 1 at 2.
8. *Ibid* at 192.
9. *Ibid* at 2.

I. EXAMINING THE EVOLUTION OF THE INCREASINGLY INDUSTRIALIZED INDUSTRY OF CYBERCRIME

The book is structured into two distinct parts. Firstly, Lusthaus outlines the evolution and nature of the cybercrime industry in general. In particular, he addresses the puzzle of how this industry was able to develop in spite of the challenges associated with the greater level of anonymity involved in cybercriminal operations. As part of his discussion related to the evolution of the industry, Lusthaus begins by defining the term "cybercrime" and establishing the scope of his study. The book "focuses on cybercrime that involves an element of profit, as opposed to cyber-activities with motivations that are more malicious, personal, or political."[10] Lusthaus provides a survey of the developments that led to cybercriminal activity evolving from being a largely informal, recreational cottage industry, to a large, illicit, and professional industry heavily driven by profit.[11] Beyond outlining the industry in a historical sense, Lusthaus analyzes the current state of cybercriminal activity by examining core aspects of how the industry has become more developed, such as its increasingly specialized nature and escalating level of professionalism.[12]

This discussion leads into the book's second part, which demonstrates the remarkable degree of cybercriminals' collaboration, cooperation, and organization, despite operating anonymously in a fundamentally distrustful environment.[13] Lusthaus covers a broad range of topics regarding how cybercriminals operate, including how they are able to leverage their online identities and how they establish trust between each other. Lusthaus also reviews commonly overlooked aspects of cybercrime, including its offline dimension and the third-party systems of governance in place that have supported its industrialization. Finally, the book concludes with a brief discussion about the impact of law enforcement in this ecosystem and potential policy solutions to address the immense issues caused by the industry.[14]

Industry of Anonymity makes many significant contributions to the study of cybercrime. The book is the culmination of a seven-year field study that involved 238 interviews with participants in the cybercrime industry located across the globe. The data obtained from these direct accounts feature some truly fascinating

10. *Ibid* at 9.
11. *Ibid* at 31.
12. See *e.g. ibid* at 66-78, 78-82 (discussing specialization and professionalization, respectively).
13. *Ibid* at 93.
14. See *ibid* at 196-203.

revelations about the underpinnings of the shadowy cybercriminal underworld and will be a cornerstone of future research in a field where empirical evidence is innately difficult to obtain. Throughout the book, Lusthaus uses his findings to explore aspects of cybercrime that have been largely overlooked in existing scholarship. One example of this includes the significant offline dimension of cybercriminal activity, including how offline contact is used by some criminal enterprises as a trust mechanism.[15] He also examines the impact of offline third parties, such as traditional organized criminals and corrupt politicians.[16] Within each discussion, Lusthaus frequently and effectively uses excerpts from his interviews to contextualize his theoretical concepts.[17] Lusthaus also succeeds in putting a human face on the complex issue of cybercrime by examining the personal and socioeconomic factors that motivate many talented individuals to pursue such illicit activities.[18] By providing concrete, accessible examples throughout the book, Lusthaus successfully illustrates the evolution and current state of the industry in a less abstract way that industry professionals and laypeople alike will be able to understand. Through the clarity of his examples and strength of his analysis, Lusthaus provides astonishing insight into the multidimensional industry of cybercrime and addresses how it has evolved into the largely unseen industrialized force that it is today.

II. POTENTIAL TOPICS FOR FUTURE RESEARCH

In *Industry of Anonymity*, Lusthaus touches upon several important topics that fell outside the scope of the study but are compelling topics for future research. The impact of policing on the industry was discussed briefly in the conclusion,[19] and Lusthaus refers to interviews with law enforcement throughout the book.[20] However, the role of law enforcement within the industry is not discussed in

15. For a discussion on how cybercriminals use offline contact as a method for establishing trust, see *e.g. ibid* at 156-64.
16. There appears to be few existing studies that focus on the offline dimension of cybercrime. For a rare example, see Jonathan Lusthaus & Federico Varese, "Offline and Local: The Hidden Face of Cybercrime" Policing: J Pol'y & Prac, online: <https://doi.org/10.1093/police/pax042>.
17. See *e.g.* Lusthaus, *supra* note 1 at 158-64. Lusthaus discusses the purpose of offline interactions in the cybercrime industry and how they are used to overcome some of the deficiencies of solely online transactions. Excerpts from interviews are used to highlight how offline interaction can provide a number of effective enforcement tools not available online.
18. See *ibid* at 75-76.
19. *Ibid* at 195-99.
20. See *e.g. ibid* at 99.

significant depth, as the perspectives of these individuals lie mostly outside the scope of the book. Lusthaus interviewed seventy-two law enforcement agents as part of this study,[21] likely gathering a considerable amount of previously unconsolidated institutional knowledge. These findings could serve as a cornerstone for further research examining how law enforcement techniques have evolved in response to rapid changes in the cybercrime industry.

The book also establishes a basic victim profile for these types of profit-driven cybercrimes but did not closely examine cybercrime from the perspective of the victim in great detail. Lusthaus interviewed ninety-seven cybersecurity experts as part of his study, many of whom presumably work closely with prominent victims of these crimes.[22] Further research could examine in greater detail how victims are affected by these crimes and how they have adapted to protect themselves from increasingly professional attacks.

Finally, Lusthaus mentions that the relevance of state actors in the global cybercrime industry is growing.[23] This was exemplified by the previously mentioned WannaCry ransomware attack, which is widely believed to have been orchestrated by the North Korean government.[24] If this type of state-sanctioned activity becomes more prevalent, further research could examine the complex ideological and geopolitical motivations behind such attacks.

Even beyond the above examples that were outside the scope of this study, there will always be a demand for updated research in this field. As Lusthaus notes, "Cybercrime is an amorphous and constantly changing phenomenon. As new technologies emerge, new attack vectors and scams become available."[25] Due to this natural advancement of cybercrime, there will always be the need for future research in order to effectively understand and mitigate the impact of this industry on businesses and consumers.

III. CONCLUSION

Even as profit-driven cybercrime becomes increasingly prevalent and costly to its victims, the concept of cybercriminal activity remains foreign to the average person. *Industry of Anonymity* provides fascinating insight into the inner mechanisms of increasingly industrialized cybercriminal enterprises. Lusthaus

21. *Ibid* at 29.
22. *Ibid*.
23. *Ibid* at 62.
24. *BBC*, *supra* note 4.
25. Lusthaus, *supra* note 1 at 60.

demystifies the complex industry of profit-driven cybercrime by presenting the findings from his extensive seven-year study in an accessible format. Readers will develop a greater understanding of the human element behind cybercrime, as the book describes in great detail the subjective experiences of a number of prominent cybercriminals. With a clearer understanding of what motivates individuals to engage in cybercriminal activity, there can be more well-informed policy discussions to determine what can be done to stem the growth of the industry responsible for causing billions of dollars in global losses. *Industry of Anonymity* represents an enormous leap forward in understanding the complex industry dynamics of profit-driven cybercrime and will certainly be a robust platform for further research.