International Journal of Cybersecurity Intelligence & Cybercrime

Volume 3 | Issue 2 Article 5

11-3-2020

Book Review: Computer capers: Tales of electronic thievery, embezzlement, and fraud. By Thomas Whiteside

Book Review, Thomas Whiteside

Follow this and additional works at: https://vc.bridgew.edu/ijcic

Part of the Criminology Commons, Criminology and Criminal Justice Commons, Forensic Science and Technology Commons, and the Information Security Commons

Recommended Citation

Nussbaum, B. (2020). Book review of Whiteside, Thomas. (1978) Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud. New York: Thomas Y. Crowell Company. International Journal of Cybersecurity Intelligence and Cybercrime, 3(2), 62-66. https://www.doi.org/10.52306/03020520QMYS9706

This item is available as part of Virtual Commons, the open-access institutional repository of Bridgewater State University, Bridgewater, Massachusetts.
Copyright © 11-3-2020 Brian Nussbaum

Book Review: *Computer capers: Tales of electronic thievery, embezzlement, and fraud.* By Thomas Whiteside

Brian Nussbaum*, College of Emergency Preparedness, Homeland Security and Cybersecurity, University at Albany, USA

Cybersecurity is a field that is consistently concerned with the new and emerging. New threat actors, the latest un-patched vulnerabilities, the big new data breach in the news, the impacts on security from emerging technologies like artificial intelligence, and the impacts on targets that are still in their formative years like "smart cities." This forward-looking nature is both appropriate and necessary given the incredible speed at which cybersecurity has grown from a niche concern for technologists to an underlying requirement for secure organizations and a resilient society. That said, it can also result in a lack of not just historical context, but also in many practitioners (particularly new or younger practitioners) being unfamiliar with earlier versions of their own field.

Professionals, be they lawyers or doctors, learn a lot about their professions what to do, what not to do, ethical considerations, being professionals by studying their historical predecessors. This need to study a fields history is not completely absent in cybersecurity. Practitioners like Richard Bejtlich (2014) have pointed to the need for historical context, and some excellent books have tackled the history of organizational developments in government (especially military and intelligence) cybersecurity, and to a lesser extent in private sector cybersecurity. Though there have been some attempts to influence this, very few students or practitioners will routinely read much of the actual historical writing about cybersecurity published in previous decades, with the probable exception of the Cuckoos' Egg by Cliff Stoll (Stoll, 2005).

Stoll's book, while exceptionally valuable for learning about the history of cybersecurity what network intrusions are, how an adversary's goals translate to behavior, how to use technology to investigate it is not alone of the books of the 20th century that are very valuable for today's cybersecurity student or professional.

*Corresponding author

Brian Nussbaum, Ph.D., College of Emergency Preparedness, Homeland Security and Cybersecurity, University at Albany, Richardson Hall 289, Albany, NY, 12222, U.S.A.

Email: bnussbaum@albany.edu

Reproduction, posting, transmission or other distribution or use of the article or any material therein, in any medium as permitted by written agreement of the International Journal of Cybersecurity Intelligence and Cybercrime, requires credit to the Journal as follows: "This Article originally appeared in International Journal of Cybersecurity Intelligence and Cybercrime (IJCIC), 2020 Vol. 3, Iss. 2, pp. 62-66" and notify the Journal of such publication.

© 2020 IJCIC 2578-3289/2020/09

This review makes the argument that Thomas Whiteside's 1978 book *Computer capers: Tales of electronic thievery, embezzlement, and fraud* is another historical work that while not as theoretically and intellectually rich as Stoll's still has much to offer, even more than forty years after its publication. There are many recent works on cybercrime, from the theoretical (Maras, 2016; Wall, 2003; Wall, 2007) to the journalistic (Goodman, 2015; Carlin & Graff, 2018), that are very important for keeping track of insights about perpetrators and the most recent scams and attacks, and students and practitioners should certainly keep current.

Whiteside's book will not tell you about what the latest strand of crypto-ransomware will do as it ransacks your machine; rather it will expose you to many cases of early attacks on data availability for extortion including a shocking number of crimes in the 1970s in which magnetic tapes or other storage mediums were physically stolen and ransomed back to companies (or attempts were made to do so). Computer Capers will not offer brilliant insight into the NotPetya attacks that initially appeared to be a ransomware campaign and turned out to be the first global data destruction attack; but again it will expose you to many early cases of data destruction attacks involving everything from magnets to screwdrivers to firearms, as well as fascinating cases like a *"French programmer"* who left behind a logic bomb in a corporate network designed to delete his employers files two full years after he had left the firm. Understanding how companies dealt with the impacts of these early attacks and managed the consequences of their data loss including innovations like backing up data, offsite storage, limiting permissions is important insight into risk management for anyone who operates in security or disaster recovery today.

The insights from Computer Capers are not just about attack types, but attackers and their motives as well. While the book does not feature state actors as adversaries (their inclusion is part of what made Stoll's Cuckoo's Egg so important and unique), every other type of attacker dealt with today is present from insiders to activists, and from white collar criminals to hackers, from corporate competitors to thieves of physical property. Attacks on computer systems as we think of them today tend to come through the Internet, but in the 1970s, that was not a vector that existed. There were attacks that came through network connections and across phone lines, but there were many more cases of localized computer theft and fraud, and literally dozens of cases of physical attacks on computers. These attacks were sometimes criminal in nature, but often politically motivated. they came from neo Luddites who felt they were losing jobs to computers, anti-war activists who bombed computing centers belonging to the military, and anti-nuclear protestors who attempted to use *"gasoline bombs"* on computers belonging to the Atomic Energy Commission.

Even the financial criminals were very creative, though many just stole or embezzled money using *"salami-style"* attacks (in which tiny percentages of transactions were rounded off or sliced and deposited into their accounts) in financial institutions or other corporations. Early computer crime though, was not just simple fraud and embezzlement. Much was made of the 2013 case in the port of Antwerp (Robertson & Riley, 2015) in which drug traffickers appear to have used insiders and malicious implants to move shipping containers around in order to facilitate the trafficking of cocaine. This was seen as innovative and impressive when it happened in 2013.

However, in the early 1970s, Whiteside reports a case of a major railroad having *"217 railroad boxcars"* rerouted by way of their computer program used to *"direct the assembly and routing of the company's boxcars which were worth millions of dollars…"* When federal authorities later recovered them, they had been painted, had the original company's markings obscured, and were on the property of another railroad to whom the criminals appeared to have rented or resold them.

Another major case involved both corporate espionage, and apparently wiretapping or listening in on corporate networks. A major oil company dispatched geologists to inspect land in Alaska that the company would have a chance to bid on. The geologists compiled data and reports on different tracts of land, which were sent from *"a keyboard terminal there"* over *"thousands of miles of telephone line to a computer at the offices of the oil company."* Later the central office, would send back *"financial analysis"* to the staff in Alaska, including information on how much they were allowed to bid for particular tracts. Following losing all of the bids on a *"suspiciously narrow margin,"* the company conducted a security assessment that determined that someone *"using very inexpensive rented electronic equipment"* had *"tapped the oil company's computer communication line."* The company believes the costs to it from that individual case *"ran into the scores of millions of dollars."*

The victims of cybercrime in Computer Capers seem eerily familiar decades later as well. In terms of recent major data breaches, few have drawn as much social and regulatory scrutiny as the 2017 Equifax breach. Some of the high-profile cases Whiteside covers involve credit monitoring services, with both Experian precursor TRW Credit Data, as well as Equifax itself having 1970s era intrusions. Interestingly, in both those cases, false credit data was inserted into the monitoring companies' systems to facilitate financial crime, rather than having data stolen or breached. While the meddling in the 2016 election, and concerns about election cybersecurity feel intensely new and modern, here too there are precursors from decades back. In 1971 a California company was sued by the state for using a computer tape of voter roll data "for commercial purposes," and in 1972 a computer operator for the New York City Board of Elections (BoE) appears to have committed voter-fraud when he submitted punch cards registering one hundred ineligible voters. More broadly, the victims of 1970s computer crimes documented in the book involve all sorts and sectors from giant global corporations like Exxon to civil organizations like The Girl Scouts of America.

Today, one of the big annual releases of information not really data per se about cybercrime is the *Verizon Data Breach Report*, an annual snapshot of some of Verizon's insight into the world of cybercrime. In much the same way that modern cybersecurity data isn't publicly available or transparent, in the 1970s too, researchers were reliant on the writing of large technology providers in order to get a sense of the scope and scale of the problem. Whiteside references, but was not able to access, what at the time may have been the biggest catalogue of computer crime in existence, an internal resource at IBM. *"…the company is said to have compiled a catalogue of more than 300 cases of computer crime…"*. The information environment around cybercrime may have improved, but elements are shockingly similar four decades on.

Whiteside's book is a work of journalism and narrative, rather than a scholarly work, so the list of chapters do not closely coincide with content; anecdotes are not grouped by type or chronology, and rather are assembled in so far as they fit into a narrative story rather than a thematic arc.

Chapter 1 "The Attenuation of Money" introduces the computerization of many aspects of life and finance, such as it was in 1978, and begins to outline some examples of early computer crime. It is important to note though, that the world in which Whiteside's book exists is not today's world.

He notes that in 1978 “Some 150,000 computers are currently in use in the United States.” And that “The number of Americans now involved in computer operations is more than two million.” While computers were growing in importance in large institutions and businesses, they were still rare things, and broad access to the Internet was still more than a decade away. That said, the utility of the stories and insights from Whiteside’s book feel surprisingly current, if indeed the technological references don’t always.

Chapter 2 “The Equity Funding Fraud” and Chapter 3 “The Union Dime Embezzlement” are large case studies of financial fraud, with insights into how cases were perpetrated, hidden, discovered, and played out. Chapter 4 “Electronic Thieves Market” is the most wide-ranging listing of cases, attack types, and organizational consequences.

Finally, in chapter 5 “Frail Auditors, Frustrated Prosecutors,” the books insights about the challenges facing investigators, auditors, companies, and law enforcement are amongst the most current and recent feeling of the books’ insights. The challenges facing organizations sound familiar. The fact that “often the crime is detected by sheer accident,” inability to consistently price or value lost or exposed information, the tradeoff between securing systems and their usability, and limited executive interest or understanding of computer security all remain timely. The law enforcement challenges largely sound familiar as well - inability to coordinate across jurisdictions, the challenges and quality of technical staff and training in law enforcement agencies, finding knowledgeable prosecutors and judges, vague laws, and challenges in acquiring and preserving evidence.

Chapter 6 “Harlowe” is probably the least effective of the book, a long case study of an embezzling case, with some insight into white collar crime, but less broadly applicable insight about computer crime. Chapter 7 “Security and Flexibility” and chapter 8 “Trapdoors and Trojan Horses” are really the chapters in which Whiteside collects many of the policy, organizational, and even technical insights about the challenges of understanding and dealing with computer crime. There are several appendices including proposed legislation addressing computer crime, a case study in a penetration of a UNIVAC computer, and most interestingly a excerpt from a 1976 General Accounting Office (GAO) report on computer crimes in US federal government programs.

The book is far from perfect as either a historical or journalistic effort. (Whiteside was a staff writer for the New Yorker when he wrote the book). Virtually none of the cases are documented there are no footnotes or endnotes, and Whiteside acknowledges changing the names of some of the individuals involved in the cases. That is, this book would not be suited to provide primary or even documented secondary source material to inform a case study for example; rather it provides a broad narrative and insights into behavior from vignettes and anecdotes. Its short bibliography is also interesting in terms of thinking about these problems of documentation; only two of its twenty references date from before 1973. This really was a book about computer crime at a time when such a thing was exceedingly tough to compile.

It is worth noting that it was not the first book on the topic. Both Gerald McKnight’s 1973 Computer Crime, and Donn B. Parker’s 1976 Crime by Computer predate Whiteside’s Computer Capers. This is really the first book that was written on the subject by a journalist (rather than a technology specialist) and for a broad audience. All three books are really listings, catalogues, and descriptions of numerous criminal episodes involving computers. One reviewer actually described Parker’s book as “an unexceptional compendium of newspaper clippings on this growing problem of ‘computer abuse’ (Rabjohn, 2015).”

While Whiteside's book has problems, it is not merely a compendium of newspaper clippings. All three books have an emphasis on financial crimes facilitated by computers and computer operators of the era (Parker, 1983), in part because as today, most computer crime is motivated financially, and in part because such crimes are more likely to be made public particularly through legal proceedings than the hacking exploits of nation states.

Both early and modern cybercrime are very interesting, and while they differ, they are not always as complex phenomena as might be thought at first glance. Whiteside paraphrases Assistant Attorney General Richard Thornburgh describing the varieties of computer crimes in 1976 *"... the computer as the victim, the computer as the environment, or the computer as the accomplice ..."* Whiteside's book provides an important insight for students and professionals into what computer crime looked like in the early years of computing, but more so into the remarkable continuities between early challenges of cybercrime and those faced today.

References

Bejtlich, R. (2014). *Strategy, not speed what today's digital defenders must learn from cybersecurity's early thinkers*.

Carlin, J. P., & Graff, G. M. (2018). *Dawn of the code war: America's battle against Russia, China, and the rising global cyber threat*. Hachett.

Goodman, M. (2015). *Future crimes: Everything is connected, everyone is vulnerable and what we can do about It*. Anchor.

Maras, M. H. (2016). *Cybercriminology*. Oxford University Press.

Parker, D. B. (1983). *Fighting computer crime*. Scribner.

Stoll, C. (2005). *The Cuckoo's egg: Tracking a spy through the maze of computer espionage*. Simon and Schuster.

Wall, D. (Ed.). (2003). *Crime and the Internet*. Routledge.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.