Shouzab Khan

CJ 502- Computer Forensics

Prof. Gary Warner

5 October 2023

The GAO Report: Challenges in Cybercrime

In June 2007, the United States Government Accountability Office (GAO) published the "Public and Private Entities Face Challenges in Addressing Cyber Threats" report. The report mentioned four major challenges to addressing cybercrime. According to the GAO, internet fraud, child exploitation, identity theft, and terrorism are a few of the criminal acts facilitated by computer interconnectivity. The advancement in computer systems has brought many benefits while simultaneously making it easier for criminals to use computers for illegal harm. Protecting networks, identifying illicit activity, conducting investigations, and prosecuting offenders are all part of the efforts to prevent cybercrime. The three main objectives of the Government Accountability Office (GAO) were to assess the effects of cybercrime on the economy and security of the country, identify obstacles to combating cybercrime, and identify the major federal, nonfederal, and private sector organizations responsible for combating the problem. GAO held talks with representatives of the public and private sectors while reviewing a wide range of papers, studies, and surveys to accomplish these goals. The GOA has also made some suggestions that the Attorney General and Secretary of Homeland Security should ensure that law enforcement agencies have modern and updated tools and skills for analysis and technology. The Federal Bureau of Investigation and the U.S. Secret Service indicated that they are already

engaged in assessing and enhancing these capabilities in their answers to an early draft of this report.

Cybercrime threatens national security and obligates the United States government to spend billions of dollars annually to mitigate the issue of cybercrime. According to an FBI report on the Security Week website, the annual loss due to cybercrimes in the United States is estimated to be around $10 billion. In their report, the GAO mentioned concerns about the constant threat to national security from other countries and terrorists. The intelligence agencies have stated that all these nation-states and terrorists can launch a coordinated cyber-attack on the United States and hack air traffic controller, electric power distribution, and banking systems. According to the FBI, terrorist organizations have used cybercrimes to raise money and defraud funds. Even though victims report cybercrime mentioning the estimated financial losses, the consolidated impact of cybercrimes remains unknown because it is not always reported and detected. According to the GAO report, both public and private entities are designated to stopping, detecting, investigating, and punishing cybercrime. Departments such as Justice, Homeland Security, Defense, and the Federal Trade Commission play critical roles in dealing with cybercrime on a national scale. Law enforcement agencies conduct similar activities at the state and local levels. Private organizations, such as internet service providers and software developers, play a significant role by developing and applying technologies to detect and prevent cybercrime, and assist in collecting evidence for investigations. There are also other collaborations in place to combat cybercrime. These collaborations can involve government agencies working together, or they can involve both public and private organizations collaborating.

Organizations face numerous challenges pertaining to dealing with cybercrime. All public and private entities are working together closely to address cybercrime challenges. Moreover, federal and legislative agencies are taking necessary steps to ensure adequate law enforcement capabilities. Some of the major cybercrime challenges mentioned in the GAO report are: reporting cybercrime, ensuring adequate law enforcement's analytical and technical capabilities, a borderless environment consisting of multiple laws and jurisdictions, and implementing information security practices and raising awareness. Reporting cybercrime means that people do not report the cybercrime to law enforcement accurately. Organizations do not report this crime for certain reasons, including fear of reputational damage, impact on the financial market, litigation concerns, signal to attackers, job security, lack of law enforcement, and inability to share information because of unawareness of resources. Ensuring adequate law enforcement analytical and technical capabilities means obtaining and retaining investigators, prosecutors, and cyber forensics examiners. It also includes staying updated with current technology and criminal techniques. Working in a borderless environment with laws of multiple jurisdictions means that cybercrime deals with criminals across borders; different countries have different laws and legal procedures which can aggravate complications. Lastly, implementing information security practices and raising awareness means protecting information systems and there is limited education and awareness of cyber threats, criminal behaviors, and resources to help report and mitigate them. According to the Reuters website, distance is one of the main differences between traditional crime and cybercrime. Cybercrime is conducted on interstate and international levels, which means that the victim, suspect, law enforcement, and evidence are no longer together under the same jurisdiction in most cases.

There are many challenges that private and public entities face, but in my opinion, the most improvements have been in reporting cybercrime since the GAO report came out in 2007. In the early 2000s, victims did not report cybercrime commonly. Another reason is the impact of declaring cybercrime on a company's financial market. If companies announce data breaches and cyber-attacks, it can potentially harm the company's stock prices and credit rating. According to CSO, companies may be reluctant to report cybercrimes because of time and expense constraints, and the lack of trust leading to the perception that reporting will not recover the business. Also, publishing the damage blemishes the organization's reputation, downgrading customer's perception of the brand. The customers will lose confidence and the competitors will use this wavering trust as an opportunity to promote their brand. Reporting cybercrime can also result in lawsuits by customers, stakeholders, and investors. Disclosing cybercrime to the public, the cyber-attack perpetrators will discover that the company defense is currently weak and may try relaunching continuous cyber-attack. Even if the organization wants to share information with the law enforcement agencies, once the investigation starts, the ability to share information gets limited. Also, sometimes the Information Technology employees may not report the attack because of the fear of losing their jobs. According to many private entities, the law enforcement agencies fail to investigate the reported cybercrimes, which discourages future reporting. Public and private entities and law enforcement agencies are trying to improve reporting of the attacks. These efforts aim to increase the reporting ratio of cybercrimes by building stronger relationships with the public and agencies. Since 2007, the challenges in the cybercrime world have improved significantly because of law enforcement agencies' continuous efforts.

Since 2007, many factors have contributed to improving cybercrime reporting. I believe one reason for this improvement is increased awareness. Over the past ten years, there has been

significant awareness in public and private entities reporting the crime because of the increased efforts of the news media, agencies, social media, and cybercrime experts who work on increasing cybercrime reporting. Also, legal regulatory changes are some of the biggest reasons for the improvement in the numbers and quality of cybercrime reporting. Since 2007, countries have introduced legal regulations for cybercrime, helping law enforcement act against criminals in a well-suited manner. Now, countries have cyber courts specially designated to deal with cybercrime-related legal matters. Also, many law enforcement and cybersecurity agencies have made changes in the reporting process such as making dedicated websites and helplines for individuals to report crimes easily. Finally, the wide availability of cyber education and training has also helped improve cybercrime reporting by enabling people to detect cyber threats and attacks easily. Advancement in cybersecurity technology has made it easier to take safety precautions against it. These examples show the changing landscape of the cyber world and the improvement in the challenges of reporting cybercrime since 2007. The challenge in the cyber world persists despite significant reporting improvements. According to the PWC, cyber breach reporting is required by law for better cyber defense. Cyber attackers get an advantage because most of the time the responders do not share the necessary information, halting immediate action, investigation, and a timely response. Reporting processes need to be efficient enough that when as soon as an attack happens, an immediate report can be filed.

I think the greatest challenge of cybercrime is working in a borderless environment with laws of multiple jurisdictions. Cybercrime is a type of crime that can be done at any place at any time. It can be done to whoever, regardless of the location. According to the CarnegieEndownment website, some countries have programs and unions where the same laws apply to international cybercrime that are applicable to any local crime. However, countries like

the United States do not share friendly relations with countries like China, Russia, North Korea, etc. Therefore, it is nearly impossible to resolve cybercrime issues with them. Tracing the criminal evidence of cybercrime can also be challenging because the criminal and the evidence are at separate locations. Anything involving cybercrime or the internet means that the entire world is included, and anyone in any country in the world can be the perpetrator or the victim. Dealing with international laws and regulations is hard because every country has different preferences, and they deal with cybercrime differently. For instance, one country can have strict laws and regulations for cybercrime, but the other country might not have any rules, letting the criminals roam freely. Technical challenges while chasing the evidence and the criminal in any other country can he hard because the evidence could be stored in different places and the laws may make arresting the criminals complicated. It is also difficult to take legal action against cybercriminals in some countries because of longer waiting times to get the documentation together. However, there are laws to help deal with cybercrimes internationally. According to the tandfonline website, “International law provides a framework for holding countries responsible for the malicious cyber activity and offers a framework for preventing escalation.” Still, there are laws that can help us deal with cybercrimes internationally.

By reading the report from GAO, I conclude that there are advancements in investigation of cybercrime. Regardless of all the progress regarding cybercrime, the cybersecurity world is facing many challenges. Producing better cybersecurity technology is one way to resolve issues related to cybercrime. Cybercrime is costing the United States and other countries billions of dollars every year. The loss is bigger than it looks because we do not know about the economic challenges that each country faces. It takes substantial funds and human capital to combat cybercrimes. Implementing all the laws that are already in place will help all countries build

better relationships in general. The public, private, and governmental entities are unaware of the exact harms of cyber security issues, but they are continuously working to resolve cyber security issues across borders. Additionally, a lack of knowledge about cybersecurity and cybercrime laws intensified the issue. Getting the countries to willingly collaborate and cooperate with other countries can resolve these issues as they can come up with coherent laws and implementation strategies. In short, the cyber world can significantly benefit from raising more awareness among people, streamlining reporting procedures, developing improved technology, and training company employees through courses and workshops, enhancing their cybersecurity skills.

References

Kovacs, B. (2023, March 13). *Cybercrime losses exceeded $10 billion in 2022: FBI*. SecurityWeek. https://www.securityweek.com/cybercrime-losses-exceeded-10-billion-in-2022-fbi/

U.S. Government Accountability Office (U.S. Gao). (n.d.-b). https://www.gao.gov/assets/gao-07-705.pdf

Bandler, J. (2023, March 21). *Solving the cybercrime problem*. Reuters. https://www.reuters.com/legal/legalindustry/solving-cybercrime-problem-2023-03-21/

Swinhoe, D. (2019, May 30). *Why businesses don't report Cybercrimes to Law Enforcement*. CSO Online. https://www.csoonline.com/article/567307/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html

PricewaterhouseCoopers. (n.d.). *Cyber breach reporting to be required by law for Better Cyber Defense*. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-breach-reporting-legislation.html

Hollis, D. (n.d.). *A brief primer on International Law and Cyberspace: June 2021*. Scribd. https://www.scribd.com/document/584711042/Hollis-Law-and-Cyberspace

Moynihan, H. (n.d.). *Full article: The vital role of international law in the framework for ...* Taylor and Francis Online. https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1832550