Policy Brief #2: Fighting Cybercrime and Ransomware

Brittany T. Searight, Gerald Jamieson, Houssam Eddine Al Tibi, and Lila Alshehri

PhD in Leadership and Policy, Niagara University

ADS 720 Process, Politics and Evaluation of Public and Social Policy

Dr. Leone

March 21, 2025

Policy Brief #2: Fighting Cybercrime and Ransomware

Executive Summary

Cybercrimes are illegal activities performed using a computer or a network. Types of cybercrime include but are not limited to Privacy Invasion, Financial Crimes such as Identity Theft, Cyber Terrorism, Cyber Exploitation such as Revenge Porn and Child Pornography, and Cyberbullying.

Ransomware is malware that encrypts, locks or threatens the release of files and demands payment to regain access. Common forms of ransomware include but are not limited to crypto ransomware, Locker Ransomware, Scareware, etc.

This policy brief will discuss the many forms of cybercrime and ransomware, along with proving policy options and recommendations to combat these issues.

Introduction and Defining the Problem

Numerous types of cybercrime exist today, all of which have detrimental effects on people's financial, mental health, and physical safety. As a result, entire nations' economies and political stability suffer (Ibrahim et at., 2021).

Cybercrime

Das and Nayak (2013) stated that cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks (p.142).

Types of cybercrime

Privacy Invasion and Identity Theft: More than ever, personal information is at danger due to digital data collecting. Social Security numbers are used by citizens and some residents of the United States for identifying purposes in the areas of work, healthcare, education, and taxes

(Sharma & Gaherwal, 2017). A person's Social Security number may facilitate identity theft and provide a wealth of information about their citizenship. It also covers the theft and access of an individual's digital credit card information (Al-Khater et al., 2020, as cited in Ibrahim et al., 2021).

Cyber Terrorism: According to Marsili (2019), cyber terrorism is the use, operationalization, or targeting of computers and networks with the intention of disseminating information or provoking fear, anxiety, or violence.

Child pornography. Disseminating child pornography is a severe crime worldwide, regardless of sociological variations. The dissemination of digital recordings (videos, pictures, and audio files) depicting children and juveniles wearing unsuitable clothing, very little clothing, or no clothing at all, as well as speaking or posing in ways that are sexually suggestive, constitutes child pornography as a type of cybercrime. The effects of child pornography on minors include disturbances in sexual development, psychiatric diseases, socialization issues, and lasting harm to one's self-image (Vyawahare & Chatterjee, 2020; Sae-Bae et al., 2014; Bada & Nurse, 2020, as cited in Ibrahim et al., 2021).

Cyberbullying: Cyberbullying is defined as when a person or group knowingly uses electronic communication and information to enable intentional and persistent harassment or threats against another person or group by sending or posting offensive text and/or images (Ramachandran, 2012). Teenagers and women are overrepresented in the victim population of cyberbullying (Vyawahare and Chatterjee, 2020).

Ransomware

Types of ransomware include railway disruptions, which are done by interfering with the railway systems. Cybercrime has the ability to stop trains. Aviation Risks, which is transmitting

false signals. Hackers may cause aircrafts to be misguided. Military Risks include private military information which can be pilfered and sent over to adversaries. Media & System Failures are Cyberattacks that have the ability to instantly bring down whole systems and stop electronic media.

Approaches and Policy Options

Option 1

It is believed that many companies do not report cybercrimes and ransomware due to the fear of reputational damage and/or legal consequences. It is vital for governments to have accurate statistics on cybercrime so that they may implement the necessary resources to combat crime. To increase reporting rates, governments can establish incentives, such as policies that offer immunity from certain liabilities.

Option 2

A second policy option to combat cybercrime and ransomware is for governments and private institutions to invest in research. Investing in research will bring awareness of the types of cybercrimes and ransomware commonly used, along with information on geographical areas and demographics of victims. With this information, proactive measures such as cyber security training can be distributed in crime hotspots.

Conclusion

The second option gives a strong way to fight cybercrime and ransomware by using research and new cybersecurity methods. When governments and private institutions invest in research, they will understand better and find optimum solutions for cyber threats. The policy focuses on making authentication methods to prevent children under 16 from having email addresses which will stop child pornography, cyberbullying, and child exploitation. When

children use email addresses that have limited access provided by their schools will make online space safer for young users. Also, stronger software security, like regular updates, strong passwords, and cybersecurity training, will help stop financial crimes like identity theft and ransomware attacks.

Creating international investigative tribunals will help different countries work together to catch cybercriminals. Using artificial intelligence in cybersecurity will make it easier to detect and stop cyberattacks quickly. Some people may worry that restricting internet access by controlling email accounts will affect digital freedom, but this step will help prevent cybercriminals from working in secret. If all countries that use the World Wide Web follow the same laws, it will make global cybersecurity stronger.

Policy Implications and Recommendations

- Research efforts to create authentication methods for children under the age of 16 to combat child pornography, cyber bullying and child exploitation.
- Enhanced software efforts such as frequent software updates, security patches, strong passwords and training and awareness courses to combat financial crimes such as identity theft and ransomware.
- Create international investigative and policing tribunals to combat cybercrime.
- All countries wishing to participate in the World Wide Web are subject to the same laws.
- Incorporate Artificial Intelligence in cybersecurity efforts.
- Restricting access to the internet by regulating the acquisition of an email address.

References

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International journal of engineering sciences & Emerging technologies*, *6*(2), 142-153.

Ibrahim, S., Nnamani, D., & Okosun, O. (2021). Types of Cybercrime and Approaches to Detection. *IOSR Journal of Computer Engineering*, *23*(5), 24-26.

Marsili, M. (2019). The war on cyberterrorism. *Democracy and security*, *15*(2), 172-199.

Ramachandran, V. S. (2012). *Encyclopedia of human behavior*. Academic Press.