

Organized crime IN CSC

Michael Amoo



DUE: April 18, 2024

CSC 120 34

Tonja Owens

Organized crime has undergone changes in times using advancements in technology to carry out cybercrimes, with greater complexity and reach. This study examines the connection between organized crime and cybersecurity looking at the characteristics of groups, types of cybercrimes committed methods used, key examples, effects on cybersecurity, future outlooks, and challenges.

To comprehend the nexus between organized crime and cybersecurity, it's essential to understand the structural underpinnings of these criminal enterprises. Organized crime groups operate akin to legitimate businesses, boasting hierarchical structures with clear leadership roles and well-defined chains of command (United Nations Office on Drugs and Crime). Moreover, these groups transcend geographic boundaries, establishing intricate global networks and collaborating with other criminal organizations to amplify their illicit activities. (United Nations Office on Drugs and Crime). Their operations are underpinned by sophisticated techniques and tools, including the development of advanced malware and the exploitation of zero-day vulnerabilities, all motivated by the pursuit of financial gain (Federal Bureau of Investigation).

The strategies employed by organized crime, in cyberspace cover a range of practices that pose significant dangers to individuals, companies, and governments alike. Various cyber crimes, including data breaches, theft, ransomware attacks, and distributed denial of service (DDoS) assaults, demonstrate how digital systems and human behavior can be exploited.

To execute their nefarious deeds, organized crime groups employ tactics designed to evade detection and maximize impact. Social engineering techniques, such as phishing and spear phishing attacks, exploit human vulnerabilities to gain unauthorized access to sensitive information. Additionally, malware development and distribution, facilitated by trojan horses and botnets, enable perpetrators to compromise systems and exfiltrate data. Exploiting software vulnerabilities, leveraging the dark web for illicit transactions, and employing money laundering techniques further augment the operational capabilities of these groups.

Examining prominent case studies provides invaluable insights into organized crime cyber attacks' modus operandi and impact. The WannaCry ransomware attack, which affected hundreds of thousands of computers worldwide, underscored the disruptive power of cyber extortion (Telegraph Media Group). The Carbanak cyber bank heist, involving the theft of over a billion dollars from financial institutions, exposed the vulnerability of the banking sector to sophisticated cyber threats. Similarly, the NotPetya cyberattack and the Sony Pictures Entertainment hack highlighted the devastating consequences of cyber warfare and corporate espionage, respectively (Telegraph Media Group).

The ramifications of organized crime on cybersecurity are multifaceted and profound. Beyond economic losses and reputational damage, these activities pose significant national security threats, undermining the integrity of critical infrastructure and governmental institutions (United Nations Office on Drugs and Crime). Furthermore, the legal and regulatory consequences of cybercrimes underscore the need for robust frameworks to deter and prosecute perpetrators effectively (Federal Bureau of Investigation).

It is essential to anticipate trends to address the evolving threats posed by cybercrime. As technology advances so do the tactics used by cybercriminals. The landscape becomes more complex with progressions, emerging regulations, and ethical considerations calling for a proactive and collaborative approach toward cybersecurity.

In summary, tackling the challenges at the intersection of organized crime and cybersecurity requires efforts, from all parties involved. By grasping the characteristics, strategies, and impacts of organized cybercrime stakeholders can better equip themselves to handle emerging threats effectively while protecting our economy and society as a whole.

# Bibliography

Federal Bureau of Investigation. *Business Email Compromise - FBI*. 21 December 2023. FBI. Website. 10 April 2024. <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/business-email-compromise>.

Telegraph Media Group. *Sony PlayStation Hack: statement in full*. 27 April 2011. The Telegraph. Website. 10 4 2024. <https://www.telegraph.co.uk/technology/sony/8476152/Sony-PlayStation-Hack-statement-in-full.html>.

United Nations Office on Drugs and Crime. *Criminal groups engaging in cyber organized crime*. 15 June 2019. Website. 11 April 2024. <https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html#:~:text=Cyber%20organized%20crime%20can%20include,typically%20associated%20with%20organized%20crime.>.