



Chapter 5

Cybercrime as a Sustained Business


Calvin Nobles

 <https://orcid.org/0000-0003-4002-1108>
Illinois Institute of Technology, USA

Sharon L. Burton

 <https://orcid.org/0000-0003-1653-9783>
Capitol Technology University, USA

Darrell Burrell

 <https://orcid.org/0000-0002-4675-9544>
Marymount University, USA

ABSTRACT

While cybercrime continues to challenge governments, businesses, and people, cybercriminals are harvesting massive payoffs by engaging in malicious operations. A significant impediment to countering cybercrime is the lack of a standardized definition of cybercrime that transcends international boundaries and hegemonic societies. The extensive taxing on law enforcement organizations to pursue cybercrime across international borders contributes to normalizing cybercrime as a sustained business. As cybercrime evolves and challenges traditional defenses, new types of cybercrime are engineered as digitalization and internet-based activity increase. Unfortunately, policies, policing, legal authorities, and prosecution of cybercrime trail the escalating cybercriminal activity. Cybercriminals are mimicking traditional business models to offer nefarious services such as cybercrime-as-a-service and customer service support. Until progressive action with legal authorization is manifested by international and national organizations, cybercrime will be a sustained business for cybercriminals.

INTRODUCTION

Cybercrime continues to impose economic, security and technological challenges on developed and less developed countries. Organizations' expanding reliance on digitalization and information communication technologies increases the probability of cybercrime (Nobles, 2019). During the pandemic, increasing employees worked from home as cybercrime reached unprecedented levels and caused chaotic disturbances for countries, businesses, and people (Monteith et al., 2021). Researchers noted that cybercrime is evolving from simple and nefarious incidents to sophisticated cyber-attacks supported and led by nation-states or illegal hacking activities (Ablon et al., 2014; Huang et al., 2018). Sixty percent of the world uses the internet resulting in increased illicit behavior involving the internet (Phillips et al., 2022). While most will agree that cybercrime is causing global havoc and disrupting international security, what is not clear is what constitutes cybercrime.

Cybercrime is a sustained business practice for malicious actors because it is a lucrative, easy, and has a low probability of getting caught (Smith et al., 2020). A critical issue is the lack of tools to calculate the magnitude and impact of cybercrime with the same exactness as traditional crimes (Caneppele & Aebi, 2017; Tcherni et al., 2016). Cybercrime is exacerbated by malicious actors capitalizing on digitization, such as developing social networks, forums, chat channels, and the dark web to exchange ideas, practices, and tradecraft (Leukfeldt & Jansen, 2020). This proposal highlights problematic areas and approbates cybercrime as a sustained business. The article emphasizes defining cybercrime, the cost of cybercrime, the role of digitalization in cybercrime, the cyber threat environment, and cybercrime as a business.

Problem Statement

Cybercrime continues to wreak havoc through a continuum of disruptiveness, geopolitical interplay, and outmaneuvering traditional security practices (Ablon et al., 2014; Huang et al., 2018; Monteith et al., 2021; Sophos, 2023). Cybercrime is evolving at a faster pace than organizations can engineer solutions. The global cost of cybercrime in 2021 was approximately \$6 trillion, and the forecasted value of cybercrime in 2022 is \$8.44 trillion, which overshadows the global investment of \$160 billion on cybersecurity services and solutions, and cybercriminals use of artificial intelligence tools to gain and maintain the technical advantage (Kuzior et al., 2022; MIT, 2019; Nguyen, 2023; Statista Research Department, 2023). The general business problem is that cybercrime is disruptive, and the lucrative nature of cybercrime perpetuates the continuation of leveraging the internet to engage in nefarious digital criminal activity—proliferating cybercrime as a sustained business model. Specifically, the business problem is that organizations will continue to influence cybercrime as a sustained business without extensive counter and defensive measures at the expense of private and public organizations. Cybercrime is unlawful, yet threat actors continue to engage in malicious activity due to the low probability of being indicted.

Purpose Statement

This research aims to explore the concept of cybercrime as a sustained business and understand the underlying factors contributing to its growth and sustainability. This statement aims to provide insights into the economic, social, and technological factors that have led to the emergence of cybercrime as a lucrative industry, the various types of cybercrime, the methods used by cybercriminals to perpetrate

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/cybercrime-as-a-sustained-business/321014

Related Content

Middleware Architecture Using SOA System

Praveen Kumar Mudgal, Shailendra Singhand Sanjay Singh Kushwah (2017). *Exploring Enterprise Service Bus in the Service-Oriented Architecture Paradigm* (pp. 1-13).

www.irma-international.org/chapter/middleware-architecture-using-soa-system/178056

Process Re-Engineering Success in Small and Medium Sized Enterprises

Jeffrey Chang, Margi Levyand Philip Powell (2010). *Business Information Systems: Concepts, Methodologies, Tools and Applications* (pp. 1272-1284).

www.irma-international.org/chapter/process-engineering-success-small-medium/44138

Theoretical Foundations of Inter-Organizational Information Systems: Towards a Framework Grounded on Seven Theories

Maria Madlberger (2012). *Inter-Organizational Information Systems and Business Management: Theories for Researchers* (pp. 33-49).

www.irma-international.org/chapter/theoretical-foundations-inter-organizational-information/61604

Information Sharing and Supply Chain Performance: Understanding Complexity, Compatibility, and Processing

Clay Poseyand Abdullahel Bari (2010). *Business Information Systems: Concepts, Methodologies, Tools and Applications* (pp. 1946-1955).

www.irma-international.org/chapter/information-sharing-supply-chain-performance/44177

A Decision Support System for ERP Implementation in Small and Medium-Sized Enterprises

Mahmood Ali, Ying Xieand Joanna Cullinane (2013). *Sociotechnical Enterprise Information Systems Design and Integration* (pp. 97-121).

www.irma-international.org/chapter/decision-support-system-erp-implementation/75877