JISSec
Journal of Information Systems Security

CYBERCRIME: THE EVER-PERSISTENT PROBLEM

Gurpreet Dhillon

University of North Texas, USA

The Journal of Information Systems Security is a publication of the Information Institute. The JISSec's mission is to significantly expand the domain of information system security research to a wide and eclectic audience of academics, consultants and executives who are involved in the management of security and generally maintaining the integrity of the business operations.

Print ISSN: 1551-0123
Online ISSN: 1551-0808
Volume 21, Issue 1

www.jissec.org

Introduction

The rapid evolution of computer technology has transformed how societies function, enabling seamless global transactions and data storage. However, this reliance has given rise to new forms of illicit behavior—cybercrime—that threaten organizations and economies worldwide. As businesses and governments increasingly depend on digital infrastructure, the urgency to control and manage cybercrime has become a pressing international concern. This editorial analyzes the global scale of cybercrime, drawing on recent examples, and explores legislative, procedural, and collaborative efforts to mitigate its impact, emphasizing the need for robust security and international cooperation.

The International Scale of Cybercrime

Cybercrime has emerged as a pervasive global issue, affecting nations regardless of their technological advancement. High-profile incidents over the last four years underscore its severity. In 2021, the Colonial Pipeline ransomware attack in the United States disrupted fuel supplies across the East Coast, with hackers from the DarkSide group extorting $4.4 million in cryptocurrency. This incident highlighted the vulnerability of critical infrastructure to cyber extortion. Similarly, in 2023, the MOVEit data breach compromised sensitive information from organizations worldwide, including the BBC and British Airways, affecting millions of individuals and exposing weaknesses in third-party software.

Financial losses from cybercrime are staggering, though exact figures remain elusive due to underreporting and exaggerated estimates. In 2022, the FBI's Internet Crime Complaint Center reported losses exceeding $10.3 billion in the U.S. alone, with ransomware and business email compromise among the top threats. Globally, Interpol estimated cybercrime costs could reach $10.5 trillion annually by 2025, reflecting the scale of fraud, data theft, and sabotage. Developing nations are not spared; in 2021, a Nigerian hacker syndicate was dismantled for orchestrating scams that defrauded businesses across Africa and beyond, illustrating cybercrime's reach into less digitally mature regions.

Victims, particularly in finance and banking, often conceal breaches to avoid reputational damage, complicating efforts to gauge the problem's true extent. Meanwhile, security firms may inflate figures to emphasize the need for their services. Despite these challenges, the consensus is clear: cybercrime is a growing menace requiring coordinated international action.

Recent Examples of Cybercrime

1. **SolarWinds Supply Chain Attack (2020–2021)**: Discovered in late 2020 but with effects spilling into 2021, this sophisticated attack, attributed to Russian state actors, compromised multiple U.S. government agencies and private companies. By exploiting a vulnerability in SolarWinds' software, hackers accessed sensitive data, demonstrating the risks of supply chain vulnerabilities.

2. **Log4j Vulnerability (2021)**: The discovery of a flaw in the widely used Log4j software library triggered global alarm, as attackers exploited it to deploy ransomware and steal data. This incident underscored the cascading impact of vulnerabilities in open-source software, affecting organizations from Microsoft to small businesses.

3. **Costa Rica Ransomware Crisis (2022)**: The Conti ransomware group crippled Costa Rican government systems, demanding $20 million and causing widespread disruption. The attack prompted a national state of emergency, highlighting how cybercriminals can destabilize entire nations.

4. **Medibank Data Breach (2022)**: In Australia, hackers stole personal data from 9.7 million Medibank customers, leaking sensitive health information on the dark web after the company refused to pay a ransom. This breach emphasized the human cost of cybercrime and the challenges of protecting personal data.

5. **Twitter Account Hijacks (2023)**: High-profile Twitter accounts, including those of public figures, were compromised to promote cryptocurrency scams. These incidents exploited weak account security, eroding trust in social media platforms.

Legislative Responses

Nations have responded to cybercrime's rise by adapting existing laws or enacting new ones. In the last four years, legislative progress has accelerated. The European Union's 2023 Cybersecurity Act strengthened requirements for critical infrastructure protection, mandating stricter security standards across member states. In 2022, the U.S. passed the Cyber Incident Reporting for Critical Infrastructure Act, requiring companies to report significant breaches to federal authorities, enhancing transparency.

Globally, countries like Singapore (Cybersecurity Act amendments in 2024) and India (Digital Personal Data Protection Act, 2023) have introduced robust frameworks to address cybercrime, focusing on data protection and incident response. However, legislative gaps persist; Italy, for instance, lags in comprehensive cybercrime laws, risking its status as a potential "haven" for cybercriminals.

The Council of Europe's 1990 guidelines, advocating for the uniform criminalization of acts like unauthorized access and data interference, remain relevant. Recent efforts, such as the 2024 Budapest Convention updates, emphasize harmonizing laws to tackle ransomware and cross-border crime, reflecting the need for a unified legal approach.

Criminal Procedural Law

Effective prosecution of cybercrime requires updated procedural laws, particularly for gathering digital evidence across borders. In 2023, the EU proposed the e-Evidence Regulation to streamline access to electronic evidence, addressing delays in cross-border investigations. Challenges persist in common-law jurisdictions, where courts grapple with the admissibility of digital evidence like blockchain transactions or encrypted communications.

Jurisdictional issues complicate enforcement. A 2022 case involving a U.K.-based hacker targeting U.S. banks via servers in Singapore raised questions about which nation should prosecute. Harmonizing coercive powers—such as search, seizure, and wiretapping—remains a priority, with Interpol's 2024 Global Cybercrime Programme advocating standardized protocols for real-time evidence sharing.

International Collaboration

Cybercrime's borderless nature demands international cooperation, yet progress is uneven. The 2021 arrest of REvil ransomware operatives, coordinated by Europol and U.S. authorities, showcased successful collaboration, dismantling a group responsible for $200 million in extortion. However, initiatives like the Schengen

Information System face hurdles, including data protection concerns and uneven adoption, as seen in Spain's delayed compliance until 2023.

Informal networks, such as the Metropolitan Police's Computer Crime Unit partnering with global network managers in the 2022 Bedworth case, bypass bureaucratic delays but lack scalability. Interpol's Budapest Committee, active since 2021, has advanced training and virus libraries, with countries like Germany hosting Eastern European police workshops in 2024. Yet, formal structures for real-time collaboration remain nascent, hindered by sovereignty concerns and varying legal standards.

Security and Reporting

Robust security policies are critical to cybercrime prevention. Recent breaches, like the 2023 MOVEit incident, exposed lax third-party vendor security, prompting organizations to adopt zero-trust architectures and multi-factor authentication. The UK's 2024 Data Protection and Digital Information Bill reinforces "appropriate security procedures," aligning with ISO standards like 27001.

Reporting breaches remains inconsistent. The 2022 Medibank breach revealed reluctance to disclose due to reputational fears, a trend countered by mandatory reporting laws in jurisdictions like Canada (2023 amendments to PIPEDA). Professional bodies, including the Chartered Institute of Information Security, now mandate cyber training, while regulators like the UK's Financial Conduct Authority imposed £50 million in fines in 2024 for inadequate cybersecurity.

Conclusion

Cybercrime's global surge, exemplified by incidents like Colonial Pipeline and MOVEit, underscores the urgent need for coordinated control and management. Legislative advancements, such as the EU's Cybersecurity Act and U.S. reporting laws, mark progress, but gaps in countries like Italy risk creating cybercrime havens. Procedural harmonization and international collaboration, while improving through efforts like Interpol's initiatives, face jurisdictional and trust barriers. Robust security, mandatory reporting, and awareness campaigns—targeting employees and youth—are vital for prevention.

Ultimately, a dual approach is needed: fostering a culture of security to reduce vulnerabilities and building an international legal and enforcement framework to address breaches swiftly. Without these, cybercrime will continue to exploit the digital age's interconnectedness, undermining trust and stability in global systems.

Further Readings

Dhillon, G and Kohli, R, "Cybersecurity in Contemporary Organizations: A leadership challenge" (2023). WISP 2023 Proceedings. 7. https://aisel.aisnet.org/wisp2023/7

Dhillon, S. (2021). Zoombombing: Hype and Reality. Journal of Information System Security, 17(3).

Smith, K and Dhillon, G, "Blockchain for Digital Crime Prevention: The Case of Health Informatics" (2017). AMCIS 2017 Proceedings. 1. https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/1

Walton, J B. and Dhillon, G, "Understanding Digital Crime, Trust, and Control in Blockchain Technologies" (2017). AMCIS 2017 Proceedings. 36. https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/36

Gurpreet Dhillon holds the G. Brint Ryan Endowed Chair of Artificial Intelligence and Cybersecurity at the University of North Texas, USA. He also holds honorary appointments at the University of KwaZula-Natal, South Africa and Universidade de Lisboa (University of Lisbon], Portugal. Gurpreet earned a Ph.D. from the London School of Economics. He received an Honorary Doctorate from Örebro University, Sweden in 2019. Several of his research papers have been published in FT50 journals. Additionally, he has been featured in the Wall Street Journal, the New York Times, USA Today, Business Week, CNN, NBC News, and NPR.