MAY 2023

THE DARK NEXUS:

Unraveling the Connection Between Financial and Cybersecurity Crime

Authored By:
Laura Whitt-Winyard, ICIT Fellow

ICIT | Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

The Dark Nexus: Unraveling the Connection Between Financial and Cybersecurity Crime

May 2023

Contents

Abstract

The Dark Nexus refers to links between financial and cybersecurity crimes. Criminals increasingly use technology for financial crimes, including targeting financial institutions for gain. Fighting the Dark Nexus requires law enforcement and financial institutions to work together through stronger regulation, improved security measures, and international cooperation. By monitoring transactions, reporting suspicious activity, and sharing information, we can cut off the flow of funds that support criminal financial and cybersecurity activities.

Introduction

The world of technology has given rise to a new kind of criminal activity: cybercrime. As businesses and individuals increasingly rely on digital systems, the potential for cybercrime has skyrocketed. However, cybercrime does not exist in a vacuum. It is closely linked to financial crime, and the two often go hand in hand.

The connection between financial and cybersecurity crime is known as the "Dark Nexus." The Dark Nexus is the intersection where the worlds of finance and technology meet. Criminals who engage in financial crimes, such as money laundering, often use technology to carry out their illegal activities. Similarly, cybercriminals often target financial institutions and individuals for monetary gain.

Examples of the Dark Nexus

One of the most common examples of the Dark Nexus is the use of cryptocurrency in money laundering. Cryptocurrencies such as Bitcoin are decentralized and largely untraceable, making them an attractive tool for criminals looking to launder money. Using cryptocurrency to transfer funds, criminals can bypass traditional financial institutions and evade detection.

For example, a criminal may use cryptocurrency to purchase luxury items like a car or jewelry. They then sell the item for cash, which can be deposited into a legitimate bank account without raising suspicion. This process effectively "cleans" the money and makes it appear legitimate.

Similarly, cybercriminals often use tactics such as phishing and ransomware to target individuals and businesses for financial gain. Hackers can access financial accounts and steal money by stealing sensitive information such as login credentials or personal data. Ransomware attacks have become increasingly common in recent years, where a hacker takes control of a victim's computer or network and demands payment to restore access.

In many cases, the victim of a ransomware attack is a business that relies heavily on its digital infrastructure. The attack can result in lost productivity, reputational damage, and financial losses. Some companies may pay the ransom to regain access to their systems, while others may rebuild their systems from scratch.

The Dark Nexus between financial and cybersecurity crime also extends to the use of the dark web. The dark web is a hidden part of the internet that is not indexed by traditional search engines and is only accessible through specific software. It is a haven for criminal activity, including selling stolen financial data, cyberweapons, human trafficking, and other illegal goods and services.

For example, a cybercriminal may use the dark web to purchase a tool or service to carry out a ransomware attack. They may also use the dark web to sell stolen financial data, such as credit card numbers or login credentials.

How to Combat the Dark Nexus

Law enforcement agencies and financial institutions must work together to combat the Dark Nexus between financial and cybersecurity crime. This requires a multi-pronged approach, including increased regulation, better security measures, AML efforts, and improved international cooperation.

Regulatory bodies must be vigilant in monitoring financial transactions, particularly those involving cryptocurrencies, to prevent money laundering and other financial crimes. In the United States, the Financial Crimes Enforcement Network (FinCEN) requires virtual currency exchanges to register as money services businesses and comply with anti-money laundering regulations. However, enforcement of these regulations can be difficult due to the decentralized nature of cryptocurrencies.

Financial institutions must also improve their cybersecurity measures, such as implementing two-factor authentication and regularly testing their systems for vulnerabilities. In addition, they must educate their customers about the risks of cybercrime and the steps they can take to protect themselves.

Criminals are increasingly using technology to facilitate their financial crimes, making it more important than ever to understand the linkages between these two types of crimes. One area where financial and cybersecurity crimes intersect is anti-money laundering (AML).

Anti-Money Laundering (AML) Explained

AML refers to regulations and procedures to prevent criminals from using financial institutions to launder money earned from illicit activities. These regulations require financial institutions to monitor customer transactions and report suspicious activity to regulatory authorities. By detecting and preventing money laundering, AML efforts can help disrupt the financial flows that fuel criminal activities, including those related to cybersecurity crime.

Here are several statistics that highlight the importance of AML efforts in combating financial crime and its links to cybersecurity crime:

- According to a report by the United Nations Office on Drugs and Crime, the amount of money laundered globally in one year is estimated to be 2-5% of global GDP, or $800 billion - $2 trillion USD.
- In 2020, the Financial Crimes Enforcement Network (FinCEN) received over 2.2 million suspicious activity reports (SARs) related to potential money laundering, up from 2.1 million in 2019.
- The World Economic Forum's Global Risks Report 2021 ranked cyberattacks as the fifth most likely risk to occur globally, with financial crises ranking fourth.

- According to a report by Cybersecurity Ventures, cybercrime damages are projected to reach $6 trillion USD annually by 2025, up from $3 trillion USD in 2015.
- In 2020, the total value of fraud losses reported by financial institutions increased by 28% compared to the previous year. (Source: LexisNexis Risk Solutions)
- The number of data breaches in the financial services sector increased by 480% between 2019 and 2020. (Source: Bitglass)
- In 2020, financial institutions reported a 67% increase in attempted cyberattacks. (Source: VMware Carbon Black)

Given these statistics, it is clear that AML efforts are critical in the fight against financial crime and its links to cybersecurity crime. By monitoring customer transactions and reporting suspicious activity, financial institutions can help disrupt the financial flows that support criminal activities, including those related to cybersecurity crime.

The Need for International Cooperation

However, the aforementioned is not enough to combat the Dark Nexus. International cooperation between financial institutions and law enforcement agencies is crucial in disrupting criminal networks that operate across borders. International cooperation is essential in combating the Dark Nexus. Criminals often operate across borders, making it difficult for law enforcement agencies to track them down. By sharing intelligence and working together, law enforcement agencies can increase their chances of catching and prosecuting cybercriminals and financial criminals.

One example of international cooperation is the Financial Action Task Force (FATF), an intergovernmental organization that sets international standards for combating money laundering, terrorist financing, and other financial crimes. The FATF has called for increased cooperation between financial institutions and law enforcement agencies to combat the Dark Nexus between financial and cybersecurity crime.

Another example of international cooperation is the Joint Cybercrime Action Taskforce (J-CAT), a partnership between law enforcement agencies from around the world, including Europol, the FBI, and Interpol. J-CAT focuses on combating cybercrime through intelligence sharing and cross-border investigations.

Conclusion

In conclusion, the Dark Nexus between financial and cybersecurity crime is a growing threat to businesses and individuals. Criminals who engage in financial crimes often use technology to carry out their illegal activities, while cybercriminals often target financial institutions and individuals for financial gain. To combat the Dark Nexus, law enforcement agencies and financial institutions must work together and take a multi-pronged approach that includes increased regulation, better security measures, and improved international cooperation. By working together, we can only hope to get ahead of the ever-evolving threat of financial and cybersecurity crime.

About the Author

Laura Whitt-Winyard is the Vice President of Security at Hummingbird. Hummingbird's compliance platform helps combat the Dark Nexus by providing financial institutions with advanced regulatory compliance tools to detect and prevent financial crimes, including those involving technology use. Its advanced analytics and monitoring capabilities can help financial institutions identify and investigate suspicious activity more efficiently and effectively, leading to faster detection and prevention of financial crime. Hummingbird's platform is designed to integrate with a financial institution's existing systems and workflows, making it easy to implement and use. This means that financial institutions can quickly and easily leverage the platform's capabilities without disrupting their existing operations.