Cybercrime vs Cybersecurity

An STS Research Paper

presented to the faculty of the

School of Engineering and Applied Science

University of Virginia

by

Michael Acolatse

April 25, 2023

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _____

Approved: _____ Date _____

Peter Norton, Department of Engineering and Society

Cybercrime vs Cybersecurity

Introduction

Digital transactions are subject to malicious activity. Through accessible technology, cybercriminals can commit financial crimes inconspicuously. In February 2018, the director of national intelligence and heads of the NSA, CIA, and the FBI warned that cyberattacks are one of the greatest national security threats (Borghard, 2018). Cybercriminals still attack the financial sector despite innovative security measures. To protect the financial sector and national security, the NSA, the CIA, and the FBI must collaborate with designated companies called Section 9 firms (Borghard, 2018).

Participants include the Cybersecurity and Infrastructure Security Agency (CISA), a federal agency that monitors US cyber and infrastructure security (CISA, 2018).CISA protects cybersecurity and infrastructure across all levels of government. Opposing them are financial cybercriminals (Ghosh, 2003). To resist cyberattacks, engineers devise new ways to detect and thwart cybercrime. As a testing method, engineers have developed a cyberattack forecasting model to protect financial institutions (Qasaimeh et al., 2022). With AI and deep learning, decision-making programs reveal patterns that engineers can use to prevent financial cyberattacks. Participants also include financial institutions, their clients, and the Internet Society, which advocates for internet resiliency and accessibility (Internet Society, 2022).

How do these participants compete online to advance their agendas? To prevent cybercrime, security efforts must understand the modes of attack. Cybersecurity protects data and intellectual property. It can prevent fraud, embezzlement and cyberespionage. It can also

improve customer confidence, protect essential hardware, and promote innovation (The Cyphere, 2020).

Government agencies have developed programs to prevent financial cybercrime (Borghard, 2018).To reach young people, CISA has partnered with nonprofits, middle and high schools, universities, and state school boards to incorporate cybersecurity concepts into classrooms (CISA 2022). Three technical attacks used by cybercriminals include hacking, malware, and DDOS attacks (Moiseienko 2018). By gaining access to sensitive information or interrupting services, they can use the interests of their victims against them. The Internet Society promotes internet education (Internet Society 2022), which can help users thwart attacks that exploit naive users. While cybersecurity agencies and social groups are better organized and have more resources than most cybercriminals, they face opponents whose methods of attack evolve rapidly and who can sometimes enlist unintentional help from naive users.

Review of Research

The research involved in this paper revolves around participants related to the problem. The sources relay information that assist in guiding my research to establish a claim. The paper Protecting Financial Institutions Against Cyber Threats: A National Security Issue. Carnegie Endowment for International Peace, Borghard, E. D. (2018) first analyzes the nature of the national security challenge then presents a case for deepening operational collaboration between the government and the sector based on existing authorities. It further proposes specific policy recommendations that could be implemented to improve defense of the financial sector against cyber-related national security threats.

The CISA provides information on government actions and education of cyber attacks and how to prevent them. My research also includes information from social groups which offer evidence on how users respond to cybercrime and spread awareness.

Jeffray and Feakin (2015) examine cybercrime's social significance and explain how technological innovations open opportunities for cybercriminals. Moiseienko and Kraft (2018) consider cybercrime's part in money laundering. Ghosh (2003) argues that cybercriminals are enabled by access and opportunity.

Current Threat Landscape and Government Responses

The financial sector is a major victim to cyber attacks. Policymakers have developed programs to prevent financial cybercrime (Borghard, 2018). Borghard mentions "in recent years, the threat landscape has evolved to encompass not only criminal or profit-motivated actors but also state and nonstate actors leveraging cyberspace to target financial institutions." States have responded by increasingly investing in developing cyber capabilities for strategic purposes. An example is the unexpected speed of the development of North Korea's cyber offensive procedures, from basic distributed denial of service (DDoS) assaults to malicious software assaults such as WannaCry in 2017. The U.S. financial system is a prime target for foreign cyber attackers due to its fundamental role in the world's economy. An assault on the financial sector could have disastrous consequences for the economy and jeopardize economic steadiness. Borghard explains "cyber attacks that disrupt critical services, reduce confidence in specific firms or the market itself, or undermine data integrity could have systemic consequences for the U.S. economy." With foreign adversaries, the issue of cyber security transcends the country's boundaries. In addition, after over two decades of global military leadership, cyberspace is the

only domain of warfare in which the United States faces near-peer, or even peer, competitors. Put together, this makes the financial sector an exceptionally attractive target for adversaries because it provides them with an asymmetric advantage (Borghard, 2018). These types of strikes bring up major issues regarding whether current strategies and abilities are good enough to protect parts of the private sector that have been selected as important infrastructure from foreign enemies. The government has been making efforts to protect from these threats. In April 2015, the U.S. Department of Defense (DOD) declared that defending the country in cyberspace was important, advancing their framework from merely exchanging information to decrease risk (Borghard, 2018). Borghard shows the Department of Defense's Cyber Strategy noted that one of their top three main objectives for their cyber mission is to "protect the nation from cyberattacks of considerable importance". This goal is independent from merely defending DOD networks and is therefore more expansive. Other than the foreign threats, aspiring cyber attackers need not create their own malicious software as they can be purchased from service providers. The UK's National Cyber Security Centre introduces a term named "cybercrime as a service"(Moiseienko 2018). With the rising accessibility of cybercrime, the response brings investigation as defined by The Financial Action Task Force (FATF) (Moiseienko 2018). With the financial sector being a major target for cyber attacks, the government and cyber security agencies continue to organize and provide security and resources.

The Escalating Challenge of Cybercrime

Cybercrime is a problem that is increasingly prevalent. A study shows the prevalence of cybercrime in different countries (fig. 1). The data shows that cybercriminals are impacting the financial sector. Identity theft (IDT) is shown to be a major tool cyber criminals use to operate.

Cybercrime *i*	Germany	United Kingdom	Netherlands	Poland	Estonia	Italy
IDT wrt. online banking (%)	1.4	3.3	1.4	1.2	1.0	1.1
IDT wrt. bank cards (%)	3.5	4.8	2.0	0.9	1.7	2.7
IDT wrt. PayPal (%)	2.0	2.3	0.7	0.8	0.4	0.9
Online shopping fraud (%)	8.4	9.0	10.3	9.7	9.1	5.0
IDT wrt. online shopping (%)	4.3	4.1	1.1	0.9	0.8	1.9
Extortion (%)	5.1	2.8	1.1	1.4	0.6	1.5
Scams (%)	5.0	4.4	2.3	3.4	1.7	2.4
Total (%)	**22.2**	**21.6**	**15.7**	**13.9**	**13.2**	**12.1**
For comparison: Malware (%)	51.5	50.5	48.8	68.1	55.7	60.1

Figure 1. Cybercrime prevalence over the last 5 years by type of cybercrime i and country j (Markus, 2018)

CISA has resources directed towards prevention of identity theft. “Unfortunately, there is no way to guarantee that you will not be a victim of online identity theft. However, there are ways to minimize your risk…”(CISA, 2022). It continues to list ways to minimize risk of identity theft and also explains how to know when their identity is stolen and what to do. A report for an international cyber policy center states, “Cybercrime can no longer be regarded as an emerging threat, but the reality of modern criminality”(Jeffray, 2015). Jeffray also says “ There have been many calls for law enforcement to do more to prevent and investigate cybercrime, yet police are often hampered in acting because of jurisdictional issues or issues inherent in such

investigations. Unlike most ‘traditional’ crimes, cybercrime intersects with multiple jurisdictions simultaneously.” It is evident that both individual opportunists and organized crime groups are committing cyber attacks, and it is not necessary to possess special knowledge in order to carry out cybercrimes. It is obvious that criminals will take advantage of opportunities presented, and such opportunities have increased recently. It was discovered that 77% of websites were vulnerable to attack with the use of toolkits found on the Internet (Ghosh 2003). With the evidence shown above it is clear that cybercrime is an issue that needs to be monitored.

Lack of awareness among some users

Despite the fact that many individuals see the internet as a safe space and utilize it frequently through their devices, numerous attacks occur every day. Even though a good amount of the effect of cyber attacks aren’t immediately harmful, the impact can be severe on a larger scale. Cybersecurity breaches can range from no or limited impact to DDoS, the stealing of data, manipulation of data, identity theft or even taking over control of systems and harming the physical world (Bruin 2017). As these attacks continue, costs of preventing and recovering increase. With the uprising of Iot devices, more users are becoming targets to cyber attacks than ever. With communication and information systems combining with the physical infrastructure, there are more networks becoming intertwined than ever before. One of the biggest threats that face naive users are malware attacks. Recent research has shown that globally, more than 200,000 malware incidents occur daily, including ransomware, phishing attacks, and malicious scans (Alzubaidi 2021). Ransomware attacks increased by 118% in the first quarter of 2019, causing severe data loss and financial implications. Comparing the first quarter results in 2020 and 2019, statistics show a 71% increase in mobile malware and 689% in PowerShell malware

(Trellix 2023). These statistics show that awareness of cyber attacks is imperative. A study was done in Saudi Arabia to demonstrate the awareness of cyber attacks. One part of the study showed that 11.7% always and 20.9% usually feel safe when accessing public Wi-Fi, and 12.6% use it regularly to access the Internet despite the potential threats of accessing public Wi-Fi. These statistics relay that these participants and their information could be at increased risk. Another part revealed that 51% used their personal information to create their passwords, and 30% never or barely changed their passwords. This shows that their accounts and devices face increased risk from attackers, as their valuable information could easily be compromised (Alzubaidi 2021). This issue can be further related to employee awareness. As organizations continue to collect more data from users, the threat of these organizations being attacked rises. A recent report explains how the lack of awareness of cybersecurity amongst employees is a tragedy waiting to strike for businesses (Worrall 2022). The report investigated employees' cybersecurity knowledge as well as how well they applied it. The researchers looked at employees from many different industries, including medical, finance, and technology. Over 50% of employees didn't think it was likely they could infect their phones with malware by clicking on suspicious links. Even worse, about 25% of all employees believe that suspicious links pose little to no threat at all (Worrall 2022). The report also showed that almost half of employees also failed to detect a phishing attempt, even though it's a common attack against businesses. These results can infer that social engineering seems to be the least understood, despite posing one of the biggest threats to many industries.

Cybercriminal resources

Cybercrime is structured around the efficient exploitation of vulnerabilities. Security teams are usually at a disadvantage because they must defend all possible entry points, while an attacker only needs to find and exploit one weakness or vulnerability (Cobb 2022). Social engineering is one of the most used methods to find vulnerabilities. Phishing and data scraping are by far the most common uses of criminal social engineering. Data scraping refers to scraping information such as email and phone numbers as well as names of people using the site. Twitter is one of the many victims of data scraping where they got the data of 400 million users and demanded payment in exchange for not selling the data (Paganini 2022). About 90% of data breaches happen due to phishing attacks (Morris 2023). There are many different types of phishing techniques. Some include: Spear Phishing, Session Hijacking, Email/Spam, and Phishing through Search Engines (KnowBe4). According to AAG global phishing statistics, Linkedin was the most imitated brand for phishing attempts. Furthermore, they found that Google blocks around 100 million phishing emails every day and about 45% of emails sent in 2021 were spam (AAG IT Services 2023). These numbers show the gravity of malicious social engineering attacks. It is also viable to conclude that these techniques can be used together. Cyber criminals can use data scraping to scrape emails and send out phishing emails.

Cybercriminals also access the dark web to help commit their crimes. The dark web provides access to a multitude of illegal sites and resources that many criminals use. The dark web provides a huge ecosystem for payment card fraud, identity theft and “cyber crime as a service” tools (CISA). One of the biggest resources in the dark web is stolen data. Stolen data tends to travel through communities, eventually landing in open forums or large marketplaces and is sold, traded, and repackaged many times (CISA). One major reason why cybercriminals

utilize the dark web is the anonymity that comes with it. The lack of proper identification presents a high risk, but it also provides an obscure sense of security that grants criminals the freedom to offer mostly illegal goods and services (Black Hat 2015). Despite the high risks associated with using the dark web, its vast network of illegal resources continues to attract cybercriminals seeking to exploit its anonymity and evade law enforcement.

Increasing Sophistication of cyberattacks

AI is recently starting to play a huge role in cybercrime. AI methods such as deep fakes and voice cloning are increasing the success rate of social engineering attacks (SoSafe 2023). Deepfakes, which combine "deep learning" and "fake media", are ideal for spreading disinformation in future campaigns as they can be challenging to distinguish from authentic content, even with technological countermeasures. This makes them especially dangerous given the widespread usage of the internet and social media platforms, as they have the potential to rapidly reach millions of people across different regions (Trend Micro 2023). Cyber criminals are also using ML to improve algorithms for guessing users' passwords. Neural networks and Generative Adversarial Networks (GANs) can empower cybercriminals to analyze large datasets of passwords and produce variations that match the statistical patterns (Trend Micro 2023). Cybercriminals are also abusing AI to imitate human behavior. Ai can bypass certain measures to catch bots to enter into systems and maliciously generate profits, collect data or skew online traffic. A forum named "nulled" was created that hosts an AI-powered Spotify bot that can imitate multiple Spotify users concurrently. The bot employs numerous proxies to evade detection while artificially inflating streaming counts, leading to increased revenue for particular songs (Trend Micro 2023). Cybercriminals are also able to weaponize AI frameworks for

hacking vulnerable hosts. This means that cyber criminals are able to hack into services or hosts automatically and are also able to automate hacking processes. All these examples and methods are proof of how cybercrime is further developing and how recent technology can also become a hindrance in combating cybercrime.

How organizations are protecting users

Technology is constantly being used by billions of people, which can leave the average user vulnerable to exploitation by criminals who have more expertise in the systems. This fact brings about groups like International Association of Security Awareness Professionals (IASAP). The IASAP is composed of member participants who are responsible for developing and implementing the security awareness programs for their respective organizations (IASAP 2023). IASAP focuses its efforts on providing the resources needed to protect organizational and customer-specific information. It also gives access to security awareness, training and educational programs from other like-minded organizations, which can help organizations stay abreast of the latest security best practices and protect user data. All of these efforts work together to help ensure that users can browse the internet with confidence that their data and information is safe and secure. The Cyber, Space, & Intelligence Association (CSIA) is an organization to provide an environment for a vital flow of ideas between national security thought leaders in government, industry, and congress focused cyber related challenges and opportunities (CSIA 2018). CSIA provides its members with access to educational, training and networking resources to stay updated on cyber security, space security and intelligence sharing. The CSIA released a report on recommendations on federal funding of R&D of the security of computer code. The report explains how cybersecurity remains a challenge due to systemic weaknesses, including exploitable code errors, critical dependencies, misaligned incentive

structures, and a complicated supply chain. To address these weaknesses, it says federal R&D spending is needed in many areas such as better code creation, cybersecurity economics, and supply chain security. CyberAngels is a program that focuses on teaching internet safety to families (CyberAngels 2022). This organization focuses on giving resources focusing on protecting against cyber threats. This method protects against the cybercriminals agenda of attacking the users trust. The organization says "our children face even greater threats in the online world – insidious because they elude detection, making them difficult to avoid." This contributes to the claim of how the naivety of users is a key factor in how cybercriminals operate. The Internet Society works to promote a safe and secure digital environment by raising awareness of cyber security and digital privacy. They host an event called The Network and Distributed System Security (NDSS) Symposium which focuses on the latest developments and research in network and distributed system security. Through the collaborative sharing of leading research on systems security they claim that the NDSS helps the internet community make the internet more secure. Richard Ford opened the event with a talk focused on ChatGPT, and what it means for machine learning for cybersecurity and privacy, and whether this will benefit defenders or provide new vectors for attackers (Internet Society, 2022). This shows the importance of raising awareness, even with regard to the newest technologies. These groups have been able to provide education that explains the ongoing cyber threats. They've also made strategies to help users identify suspicious activity and have developed methods to detect and respond to cyber threats quickly. These have helped spread awareness about cyber security and contribute to a safer cyber space.

Conclusion

It has been discussed how efforts towards cybersecurity have been improving as technology advances. Even with the increasing issue of cybercrime, the government and social groups have contributed to keeping the safety on par. As the issue of adversaries whose attack strategies toward unsuspecting users continues, the need for continual education and awareness of cyber security threats is prevalent. With the resources available and recent development of technology, cybercrime has been increasing in sophistication which is contributing to the battle in cyberspace. Through collaborative efforts of the government, private sector, and social organizations, individuals can be provided with the resources to protect themselves and their organizations from cybercrime.

References

AAG IT Services (2023). The latest phishing statistics https://aag-it.com/the-latest-phishing-statistics/

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7841324/

Black Hat (2015) CyberCrime in the deep web. https://www.blackhat.com/docs/eu-15/materials/eu-15-Balduzzi-Cybercrmine-In-The-Deep-Web.pdf

Bruijn, H. de, & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. Government Information Quarterly. https://www.sciencedirect.com/science/article/pii/S0740624X17300540

Borghard, E. D. (2018). Protecting Financial Institutions Against Cyber Threats: A National Security Issue. Carnegie Endowment for International Peace. JSTOR

CISA (n.d.). Cybersecurity and Infrastructure Security Agency.

CISA. (n.d.). The dark web and cybercrime. https://www.cisa.gov/sites/default/files/publications/202007231300_Dark_Web_Cybercrime_TLP_White.pdf

Cobb, M. (2022). 13 common types of cyber attacks and how to prevent them. Security. https://www.techtarget.com/searchsecurity/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them

CyberAngels. (n.d.). https://www.cyberangels.org/about/

Cyber, Space and Intelligence Association. (2018, March 19). https://cyberspaceintel.org/

Ghosh, A. (2003). Sizing the Opportunity for Opportunistic Cybercriminals. *Journal of Information Warfare, 2*(1) , 80–89. JSTOR

International Association of Security Awareness Professionals. (2023, January 18). https://iasapgroup.org/

Internet Society. (2022, July 12). https://www.internetsociety.org/

Jeffray, C., & Feakin, T. (2015). Underground web: The cybercrime challenge. Australian Strategic Policy Institute. JSTOR

KnowBe4. (n.d.). Phishing. KnowBe4. https://www.knowbe4.com/phishing

Moiseienko, A., & Kraft, O. (2018). The Financial Dimension of Cybercrime. In From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime (pp. 7–22). Royal United Services Institute (RUSI). JSTOR

Morris, E. (2023). How do cyber criminals obtain sensitive information? Data Science Central. https://www.datasciencecentral.com/how-do-cyber-criminals-obtain-sensitive-information/

Paganini, P. (2022). Updated: Data of 400 million Twitter users up for sale. Security Affairs. https://securityaffairs.co/139993/data-breach/twitter-400-million-users-leak.html

Qasaimeh, M., Hammour, R. A., Yassein, M. B., Al Qassas, R. S., Torralbo, J. A., & Lizcano, D. (2022). Advanced security testing using a cyberattack forecasting model: A case study of financial institutions. *Journal of Software: Evolution and Process*. https://doi.org/10.1002/smr.2489 [Original source: https://studycrumb.com/alphabetizer]

SoSafe (2023) The top 8 cybercrime trends. https://sosafe-awareness.com/resources/reports/cybercrime-trends-2023/?utm_term=cyber+crime&utm_campaign=USC_EN-Search-Non-branded&utm_source=googlesearch&utm_medium=paid&hsa_acc=2315609737&hsa_cam=19757849939&hsa_grp=147673882318&hsa_ad=650660528847&hsa_src=g&hsa_tgt=kwd-49888553&hsa_kw=cyber+crime&hsa_mt=p&hsa_net=adwords&hsa_ver=3&utm_content=https%3A%2F%2Fsosafe-awareness.com%2Fresources%2Freports%2Fcybercrime-trends-2023%2F&gclid=CjwKCAjw9J2iBhBPEiwAErwpeW0POXEYepJe5smJ2dPs6PWZlx4w9-BcIJaAyWQhCxcE6Gg8D7z4eBoCkz4QAvD_BwE

The Cyphere. (2020). Benefits of cyber security: Advantages for Businesses and Individuals. https://thecyphere.com/blog/benefits-of-cyber-security/

Trellix (2023). The Threat Report. https://www.trellix.com/en-us/advanced-research-center/threat-reports/feb-2023.html

Trend Micro (2023). Exploiting ai: How cybercriminals misuse and abuse AI and ML. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploiting-ai-how-cybercriminals-misuse-abuse-ai-and-ml

Worrall, W. (2022). Lack of employee awareness of cybersecurity is a catastrophe waiting to happen. Hacked.com. https://hacked.com/lack-of-employee-awareness-of-cybersecurity-is-a-catastrophe-waiting-to-happen/