computers

MDPI

Article

The Historical Relationship between the Software Vulnerability Lifecycle and Vulnerability Markets: Security and Economic Risks

Abdullah M. Algarni

Computer Science Department, King Abdulaziz University, P.O. Box 80200, Jeddah 21589, Saudi Arabia; amsalgarni@kau.edu.sa; Tel.: +966-12-6952000

Abstract: Vulnerability lifecycles and the vulnerability markets are related in a manner that can lead to serious security and economic risks, especially regarding black markets. In the current era, this is a relationship that requires careful scrutiny from society as a whole. Therefore, in this study, we analyzed the actual data relating to vulnerability-regulated markets in the case of two well-known browsers, Firefox and Chrome. Our analysis shows that financial reward is the main motivation for most discoverers, whose numbers are increasing every year. In addition, we studied the correlation between vulnerability markets and the vulnerability lifecycle from many perspectives, including theoretical concepts, and statistical approaches. Furthermore, we discussed the potential risks for people and organizations in terms of security and economics. We believe that money is the main motivation in vulnerability markets and that the latter are, in turn, the main driver of the vulnerability lifecycle, which presents several risks to the software industry and to society itself. Thus, in our opinion, if vulnerability markets can be controlled, the vulnerability lifecycle will be reduced or eliminated, along with its associated risks.

Keywords: software vulnerability; vulnerability lifecycle; vulnerability markets; software security; risk management; security economics

Citation: Algarni, A.M. The Historical Relationship between the Software Vulnerability Lifecycle and Vulnerability Markets: Security and Economic Risks. *Computers* **2022**, *11*, 137. https://doi.org/10.3390/computers11090137

Academic Editor: Paolo Bellavista

Received: 3 August 2022
Accepted: 6 September 2022
Published: 14 September 2022

1. Introduction

The subject of software security has emerged as a primary concern [1] and has once again been raised by individuals and government agencies in terms of risks of violations regarding information security, cybersecurity [2], and the consequences for the economy, especially in relation to attacks from actors with special agendas. Therefore, software vulnerabilities have major effects on the developmental paths of technology, development, and investment [3].

A vulnerability is established when a code or specification error occurs. Therefore, the possible vulnerability lifecycle has many phases including discovery, disclosure, patching, and exploitation. These phases have several impacts, particularly discovery and exploitation, that could be critical phases for determining the degree of risk involved. Potential vulnerability exploitations will have a major economic impact on the software industry, including software vendors and end users (i.e., individuals and organizations). A data security breach can cause a loss of confidentiality, including leaks to groups deemed dangerous to society, leading to direct and indirect cost losses [3,4].

There is a relationship between the number of code development changes in such software, resulting from software development methods and the probability of discovering software vulnerabilities that can lead to changes in the software security [5]. Therefore, vulnerability disclosure policies that release patches for those discovered vulnerabilities are key to reducing the impact on security and the economy, especially if the disclosure is made by reliable agencies, since it has a direct effect on the vendor patch time [6]. If the vulnerabilities are not patched by the software vendor, zero-day exploits will have been

identified, and the related security risks of vulnerability exploitation and disclosure will have increased [7]. Some studies have been conducted on the vulnerability lifecycle and the major players in a security ecosystem involving discovery motivations, along with search tools, vulnerability markets, criminals, vendors, security information providers (SIPs), and the public, based on thousands of publicly disclosed vulnerabilities [8].

Financial rewards are often the primary motivation for discoverers looking to detect vulnerabilities, and are frequently the reason for attacking people and organizations. Therefore, the discovery phase is becoming the main phase to focus on, since it has the most impact on vulnerability markets. Private organizations, and even several governments, now participate in vulnerability markets where vulnerabilities are traded. Vulnerability markets have expanded to include legitimate, grey, and black markets [9,10]. Legitimate markets are encouraged by creating vulnerability rewards programs (or bug bounty programs), especially in the investigation of crowdsourcing vulnerability discovery events [11] and the protection of smart cities and e-governments that use the Internet of Things (IoT) against any potential security attacks [12,13] by investigating alternative economic solutions, encompassing everything from incentive systems to market-based solutions [14]. The average cost of running these reward programs for a year is currently less than the cost of recruiting two additional software engineers [15]. In addition, vulnerability rewards programs reduce the risks associated with using different types of markets, such as black markets, where discoverers can maximize their incentives and the main customers intend to use these vulnerabilities to attack specific targets for money. From this perspective, encouraging the establishment of many reward programs will minimize black transactions and their implications, and these programs can play a great role in supporting cybersecurity [16,17]. Based on this idea, searching for new, effective, and worthy vulnerability rewards based on a modern economics model should fill the gap between these types of markets [18,19].

Many studies illustrate that each phase of the vulnerability lifecycle is likely to have a correlation with some types of vulnerability markets, and that this can produce some risks to economics and security. For example, Munaiah and Meneely [20] demonstrated, using empirical analysis, the weak relationship between the Common Vulnerability Scoring System (CVSS) and reward incentives based on 703 vulnerabilities across 24 products. However, Burkart and McCourt [21] and Allodi [22] conducted a study on the economics of vulnerability exploitation based on data collected from a cybercrime market. They found strong evidence of a correlation between vulnerability market activities and the probability of exploitation, which led to varying exploitation prices.

Other studies have strongly focused on the response of vendors' patching behaviour with regard to the impact of vulnerability disclosure threats and the presence of competitors [23]. Anderson et al. proposed 15 policies that tackle issues related to information security and that affect the security economics of the European Union [24]. In addition, they encourage internet service providers (ISPs) to take serious steps in terms of cleaning infected devices and taking care of all information or databases that contain cybersecurity incidents as well as breaches that hugely impact economics [25]. Even the reporting of software vulnerabilities in products can adversely affect the software vendors' market value [26].

This paper focuses on studying the current situation of vulnerability markets by investigating the following research questions:

RQ1: What do the actual data show about the financial transactions involved in vulnerability markets? (i.e., is money the main motivation for discoverers? Has the outsider discoverer trend increased yearly?).

RQ2: Is there a relationship between the software vulnerability lifecycles and software vulnerability markets?

RQ3: What are the security and economic risks associated with, and what is the impact of, the relationship between the vulnerability lifecycles and vulnerability markets?

The paper is organized as follows: Section 2 provides some background concepts. Section 3 presents the collected data methodology for each vulnerability associated with

the Firefox and Chrome browsers, including assigning a reporter's name and vulnerability market type. Section 4 provides a study of the monetary rewards in the vulnerability market type, offers proof of the relationship between vulnerability markets and the movement of the vulnerability lifecycle, and analyzes the impact of their security and economic risks on the consequences of that relationship. In Section 5, the problems and recommendations and the threats of validity identified are discussed. Finally, some conclusions and future work objectives are presented in Section 6.

2. Background

This work mainly focuses on understanding two major concepts: the software vulnerability lifecycle and software vulnerability markets. They are briefly described in the following sections.

2.1. Vulnerability Lifecycle Phases

The vulnerability lifecycle model [27,28] shows how a vulnerability evolves over time. The lifecycle of a vulnerability is divided into phases based on distinctive points in time, where each of them indicates a state and an associated risk [27]. Thus, the term vulnerability lifecycle denotes a fixed and linear progression from one phase to the next in order to comprehend vulnerability behavior. The following have been addressed as possible states of vulnerability:

- Birth: this refers to the occurrence of a software defect or flaw.
- Discovery: the vulnerability in the software product is discovered. The vulnerability discoverers can be either black hats or white hats.
- Disclosure: the discoverers have the option of exposing the details of the vulnerability to the developer or to the general public.
- Correction (patching): the vulnerability is fixed by releasing a software modification through software vendors or developers.
- Publicity: a vulnerability can be made public in different ways. Scripting (exploitation): anyone with moderate skills can successfully exploit a new vulnerability.
- Death: this state occurs when the vulnerability has been patched or the attackers have lost interest.

Vulnerability lifecycle discussion can aid the development, deployment, and maintenance of software systems, as well as the formulation of future security rules and the auditing of previous incidents. As a result, security concerns regarding different software products from various vendors can be assessed [29].

The sequence states of exploitation, disclosure, and patching are not always fixed [30] as sometimes the exploitation and patching can occur at a time that is earlier than, at the same time as, or after the disclosure state.

2.2. Vulnerability Market Types

Depending on the motivation of vulnerability discoverers, different types of vulnerability markets emerge. Algarni and Malaiya [9] studied discoverers' motivations and described current vulnerability markets where sellers (discoverers) and buyers (consumers) trade vulnerability.

In general, vulnerability markets are divided into legitimate (including regulated and unregulated markets) and illegitimate markets. A brief description of these is provided below.

2.2.1. Regulated Vulnerability Markets

These are controlled by conventions and laws to prevent any non-suitable actions against society as a whole. These types of market include the following:

- Publicity: the discoverer submits the vulnerability to an authority, such as software developers. money or a reward is not the main motivation for the discoverers. They always focus on building their reputations as capable researchers.

- Captive market: the discoverers belong to organizations. Thus, they are not allowed to reveal the discovered vulnerabilities externally.
- Vulnerability rewards from vendors: the discoverers can sell their findings directly to software vendors through some current rewards programs. These programs provide a good and legitimate option for discoverers to obtain rewards as opposed to resorting to other illegitimate alternatives.
- Rewards by security service companies: these companies discover a vulnerability for two main reasons: to provide a high level of security for their subscribed customers or to sell the vulnerability to software developers only.

2.2.2. Vulnerability Gray Markets (Brokers)

These are considered a legitimate market but are partially regulated by some general rules. A broker may sell a vulnerability to software developers or to some government agencies depending on who can pay more.

2.2.3. Online Forums

These online places are classified as an illegitimate market because the main objective of these forums is to exchange vulnerability information and exploit hacktivists, who plan to attack specific organizations globally, achieve a special agenda, or send specific messages, such as when the LulzSec group attacked several global websites in 2011. Thus, money is generally not the main goal in these cases.

2.2.4. Vulnerability Black Markets

These are not regulated and are therefore illegitimate markets because they are not controlled by any rules or laws. Thus, any unknown groups or organizations can buy zero-day vulnerabilities that might harm targeted organizations in several countries. Many black markets or forums exist solely to facilitate underground transactions for the exchange of malware, information theft, and other services [31]. Therefore, the vulnerability price paid to discoverers is much higher than in other vulnerability markets, and this will encourage them to sell their vulnerabilities in these black markets, which is the main risk source.

3. Methodology

We focused on the available dataset of reported vulnerabilities for Mozilla Firefox and Google Chrome that were collected by Finifter et al. [32] for the period 2009 to 2012, who analyzed cost-effective mechanisms for finding security vulnerabilities and had experts review the information for both browsers (Tables 1 and 2). We used the same dataset and methodology, such as focusing on the vulnerabilities that affect stable releases and ignoring other releases, as the basis for this work. The dataset fields detail the severity of the vulnerability, reward amount, reporter name, report date, and the type of reporter or discoverer (i.e., internal or external organization).

Table 1. Observations included in the Firefox dataset.

Severity	2009		2010		2011		2012	
	Discovery	Rewards	Discovery	Rewards	Discovery	Rewards	Discovery	Rewards
Low	4	0	6	0	3	0	2	1
Medium	5	0	13	1	24	4	23	4
High	1	0	12	4	24	10	42	24
Critical	24	0	109	24	140	39	117	79
Unknown	1	0	4	0	8	0	46	0
Total	35	0	144	29	199	53	230	108

Table 2. Observations included in the Chrome dataset.

Severity	2009		2010		2011		2012	
	Discovery	Rewards	Discovery	Rewards	Discovery	Rewards	Discovery	Rewards
Low	30	0	67	0	48	0	80	1
Medium	21	0	42	8	86	26	139	38
High	35	3	184	86	286	179	288	127
Critical	3	0	10	6	14	9	5	5
Unknown	0	0	0	0	2	2	6	11
Total	89	3	303	100	436	216	518	182

However, to understand the motivation of those discovering vulnerabilities and whether the number of yearly external reporters had grown (RQ1), we added some information to that dataset regarding vulnerabilities in both browsers to provide more data about the monetary rewards and determine what drives these vulnerabilities. For example, we used a common vulnerability and exposure identifier (CVE-ID). This provided a reference number for each vulnerability that helped obtain more significant information about it and the reporters' information, including names and organizations, by visiting databases with security vulnerabilities or trusted websites. Then, we attempted to determine the type of vulnerability market to which the reporter might belong depending on the availability and reliability of the above information, and according to the following description of a regulated vulnerability market:

- Captive market: discoverers (reporters) belong, officially or voluntarily, to Mozilla or Google.
- Vulnerability reward programs (VRPs): reporters can sell their discovered vulnerabilities directly to Mozilla or Google. This may include someone who works in a security company and individually reports a vulnerability. They receive a reward.
- Security service companies: they may discover and sell vulnerabilities to software developers (Mozilla or Google). This may also include people working for security companies who submit vulnerabilities using their own names and companies.
- Publicity: reporters may not fall into one of the above categories. This may include someone who works at a security company and individually reports a vulnerability. They do not receive a reward.

To answer RQ2, we discussed how all the main activities of vulnerability markets, such as buying and selling vulnerabilities, happen during the discovery phase. This can lead to more discussions on and analysis of the correlation between vulnerability rewards and the vulnerability movement during the well-known vulnerability discovery phase, and studying that correlation and its impact assessment based on certain market factors (RQ3).

4. Results

To investigate the research questions, we analyzed the dataset to determine the vulnerability market types. We then examined the relationship between the vulnerability lifecycle and vulnerability markets. Finally, we studied the expected impact on security and economic risks resulting from the interaction between the vulnerability lifecycle and vulnerability markets.

4.1. Money and Its Impact on the Movements of Vulnerability Markets (RQ1)

Based on our previous work [9,10], monetary transactions or the desire for money is the main reason why vulnerability markets continue to exist. Thus, proof of the types of vulnerability markets to which vulnerability discoverers might belong is needed for the analysis. We analyzed the datasets of both browsers to answer the main questions: to which vulnerability markets do the discoverers belong? Did the vulnerability markets that are interested in money increase in size yearly during the period covered by the dataset? The answers to these two questions will lead to knowledge about the percentage of discoverers

who report or sell vulnerabilities to software vendors and their monetary motivation. To this end, we provide the following analysis.

4.1.1. Vulnerability Market Share

Studying the vulnerability markets will help identify the market types within which the discoverers intend to sell their discovered vulnerabilities. The choice of vulnerability market depends on the market's attractive factors and the discoverer's motivations. We focused on regulated markets because other data are not available or are generally insufficient.

As shown in Figures 1 and 2, 31.34% and 39.76% of the vulnerabilities with high and critical severity in Firefox and Chrome, respectively, were traded in other vulnerability markets. This means that around one third of the vulnerabilities were discovered by outsiders who were looking to obtain money immediately or in the near future. The percentage of vulnerabilities discovered by captive markets was 68.66% in Firefox and 60.24% in Chrome. Rewards programs were the second largest market after the captive market for both Firefox and Chrome (30.70% and 36.97%, respectively). The publicity market was the smallest market because the severity of the vulnerabilities were high and critical, which can also apply to the current rewards programs. However, it is not clear why the security service companies' markets do not possess a proportion of the vulnerabilities at this level.

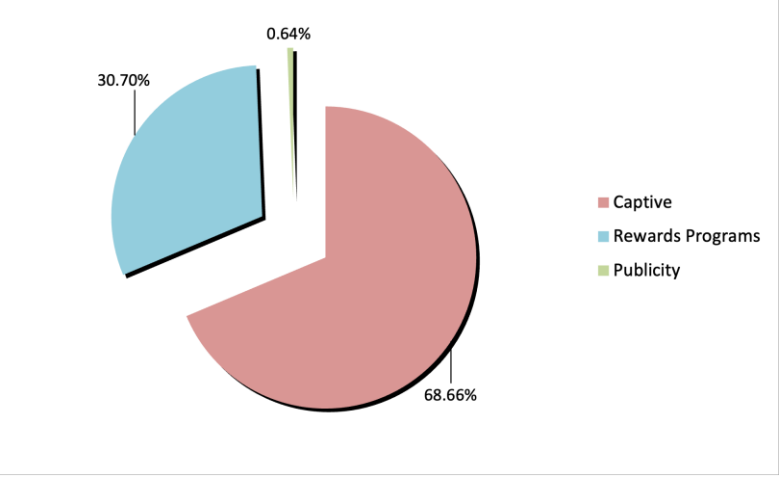

Figure 1. Firefox vulnerability market share (high and critical).

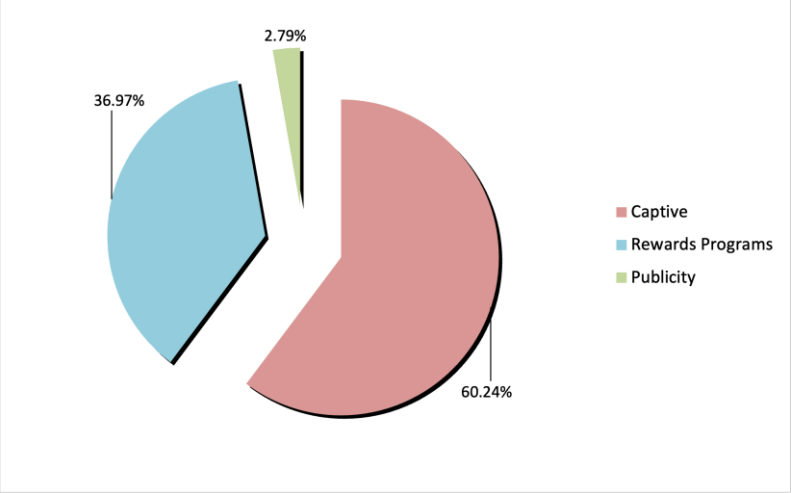

Figure 2. Chrome vulnerability market share (high and critical).

Concerning high and critical vulnerabilities, the share of captive markets mostly decreased over time for Firefox; this is probably because their proportion was taken by other markets, but the share of rewards programs mostly increased over the different years (Figure 3). On the other hand, for Chrome, the shares of captive markets and security companies increased slightly year on year, but the share of rewards programs was more volatile and decreased after the second quarter of 2011 (Figure 4). The publicity market remained fairly constant during the period studied.

For both browsers, the shares of all the markets fell in the fourth quarter of 2012, and this may be because the software quality of the two browsers improved.

4.1.2. Submarkets of Vulnerability Rewards Programs

Focusing on the rewards program markets will allow us to understand the number of and trends regarding rewarded vulnerabilities (for all severity levels), and to which vulnerability markets the discoverers who are interested in money belong to within the rewards program markets.

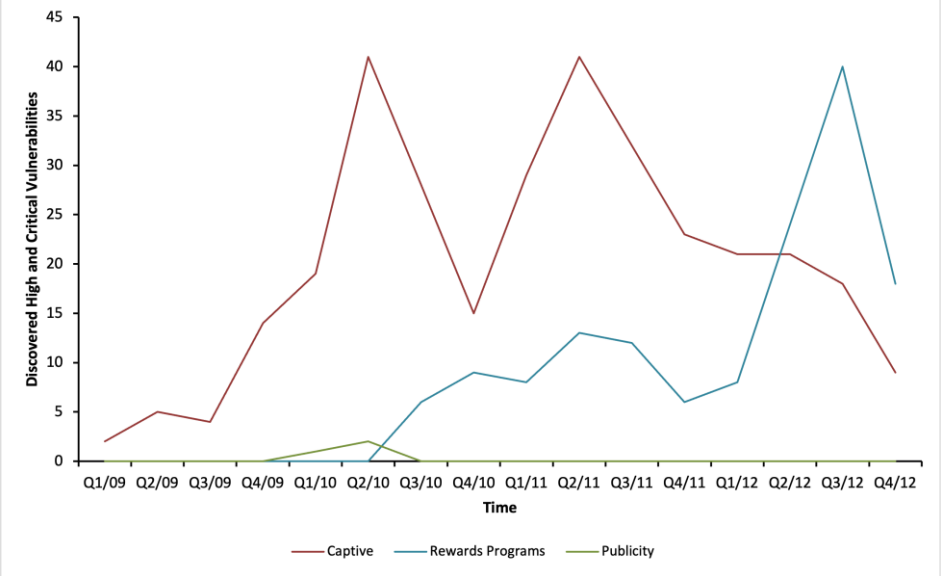

Figure 3. Trends in Firefox vulnerability discoverer types (high and critical).

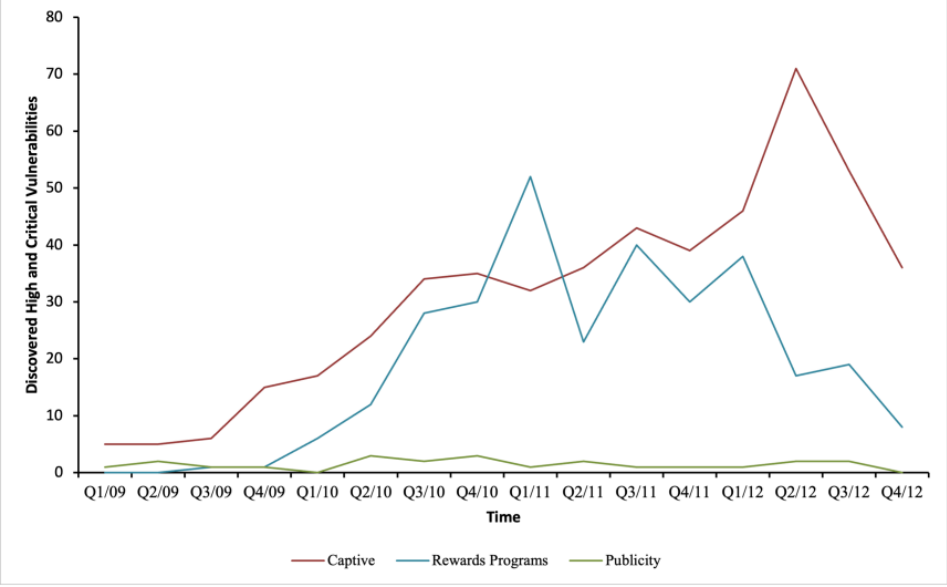

Figure 4. Trends in Chrome vulnerability discoverer types (high and critical).

When we divided the rewarded vulnerabilities into the regulated markets, there were no captive markets because Firefox or Chrome employees cannot participate in their own rewards programs. However, the share of publicity markets was almost 100% for both Firefox and Chrome (Figures 5 and 6). This means that vulnerability discoverers are looking for money or rewards, and then that these rewards programs are constantly moving.

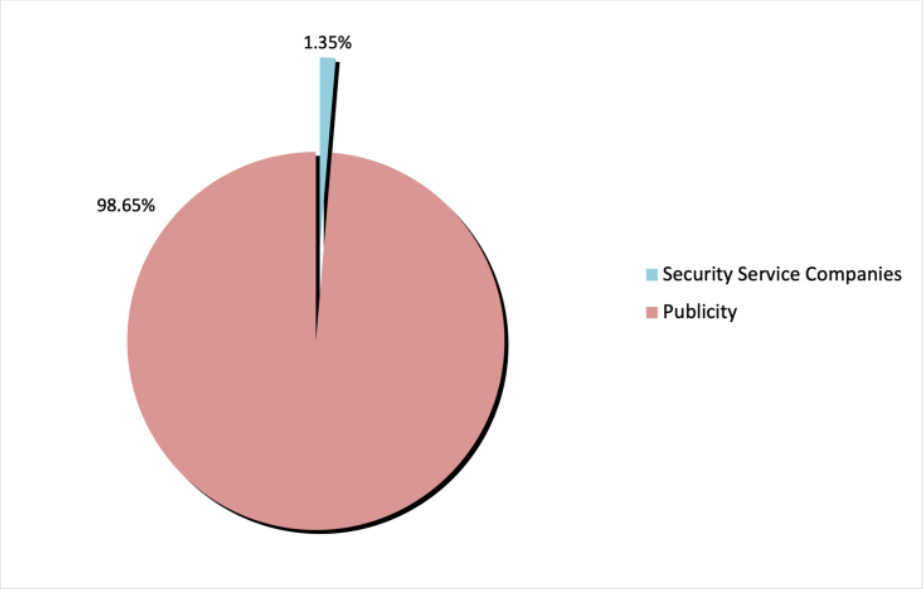

Figure 5. Firefox submarkets of vulnerability rewards programs.

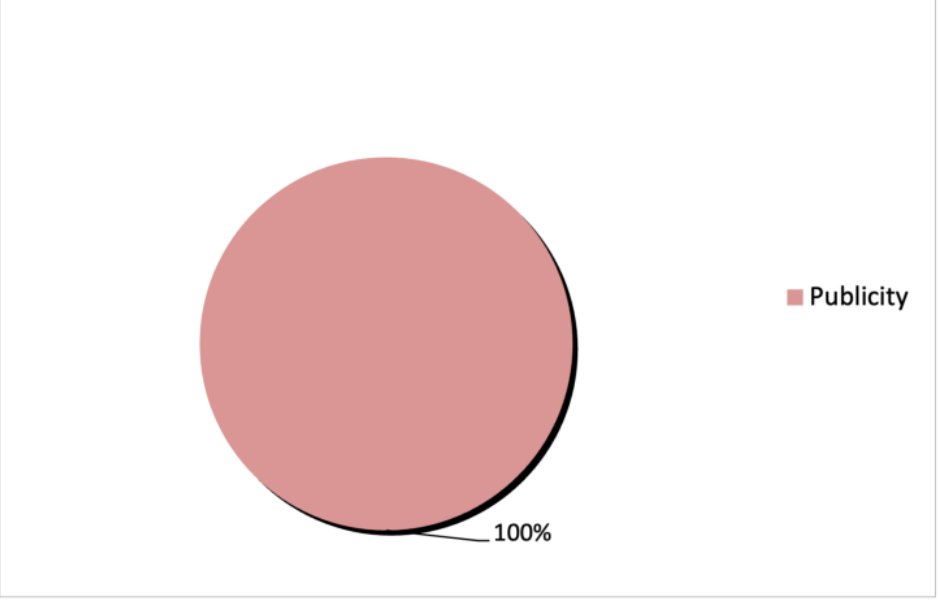

Figure 6. Chrome submarkets of vulnerability rewards programs.

The share of publicity increased almost yearly in Firefox, more so than in the case of Chrome, for which the number of vulnerability rewards programs sometimes increased but was also seen to decrease (Figures 7 and 8).

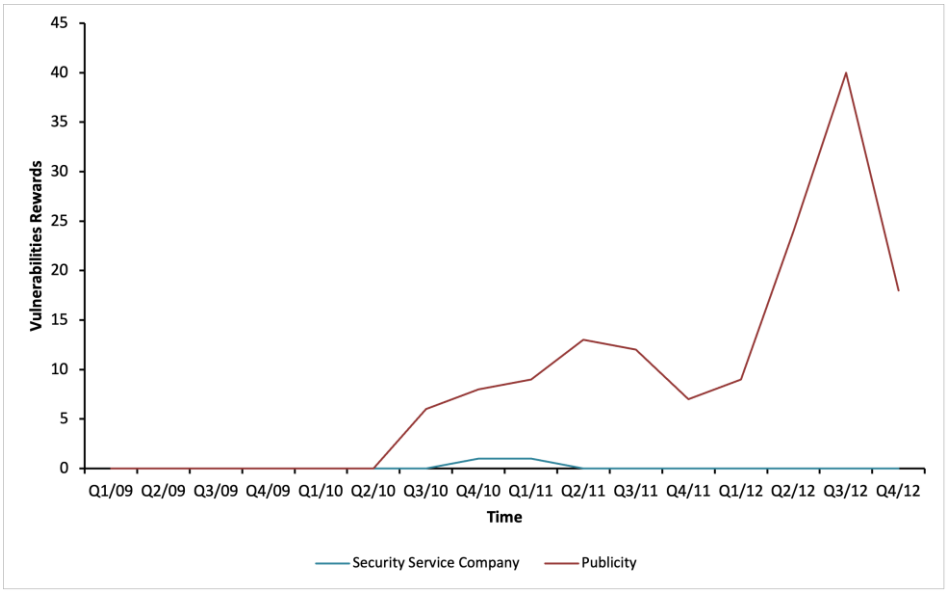

Figure 7. Trends in Firefox submarkets of vulnerability rewards programs.

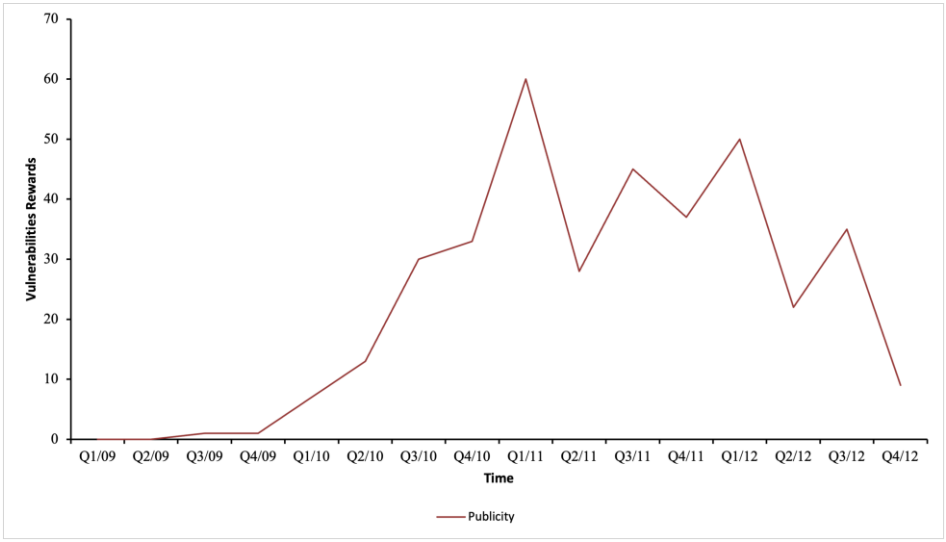

Figure 8. Trends in Chrome submarkets of vulnerability rewards programs.

4.1.3. Amount of Vulnerability Rewards

As mentioned in [9], money is the main motivation for most vulnerability discoverers. Therefore, studying the yearly money movements for both browsers is helpful since the amount of money spent on vulnerability rewards indicates that these rewards programs are successful and attractive to both sellers (discoverers) and buyers (consumers).

Stable vulnerabilities were rewarded more than non-stable vulnerabilities in Firefox ($444,000 compared to $570,000) and Chrome ($392,766 compared to $579,605). For both browsers, the reward amount for stable vulnerabilities increased more than that of non-stable vulnerabilities.

The trend in the reward amounts for the publicity markets showed the biggest increase for Firefox (Figure 9), while with regard to Chrome, they sometimes increased and sometimes decreased, depending on the severity impact (Figure 10).

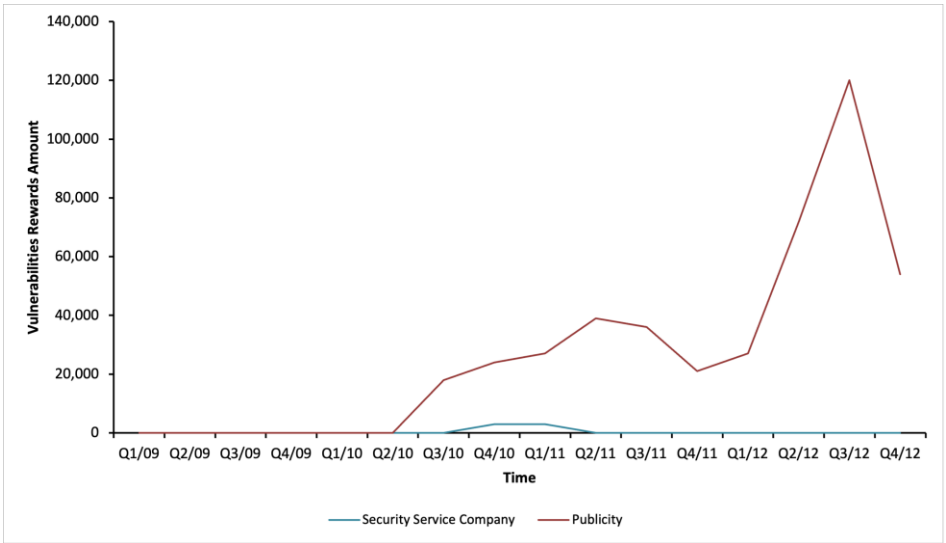

Figure 9. Trends in Firefox reward amounts of vulnerability rewards programs.

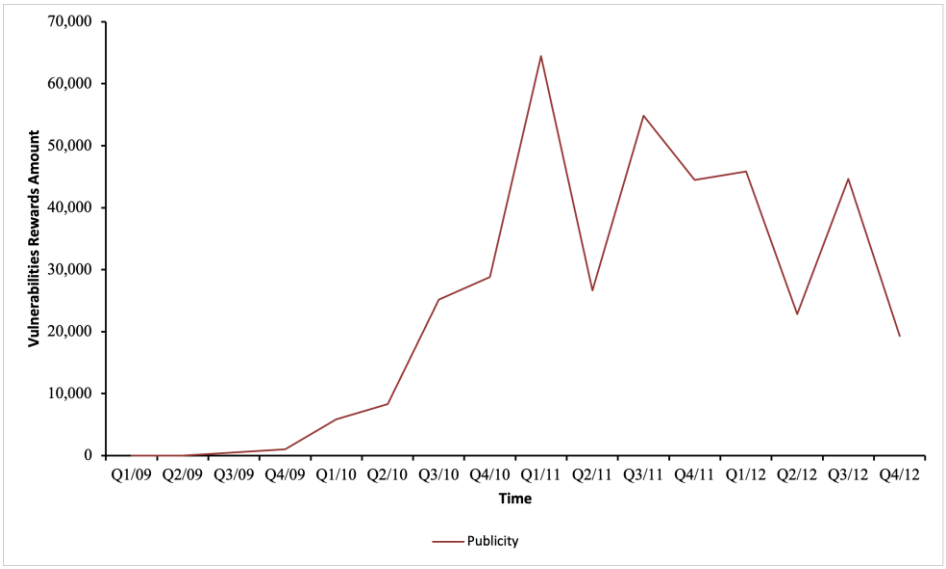

Figure 10. Trends in Chrome reward amounts of vulnerability rewards programs.

4.2. Vulnerability Market-Driven Vulnerability Lifecycle (RQ2)

In this subsection, we model the relationship and interactions between vulnerability markets and the vulnerability lifecycle. Then, we study that relationship in each main phase of the vulnerability lifecycle for vulnerability markets in general and for some specific markets, such as black markets.

4.2.1. Main Motivation of Vulnerability Discoverers

Monetary rewards are the main motivation for most vulnerability discoverers. We obtained some data about their motivations through a survey published in [9]. We found that money and its transactions are the main factors driving the different types of vulnerability markets, and it is from these that the phases of the vulnerability lifecycle will be derived. Here, discoverers are mostly white hats, and they deal with regulated markets.

4.2.2. Modeling the Relationship between the Vulnerability Lifecycle and Vulnerability Markets

To determine the relationship between the vulnerability lifecycle and vulnerability markets, we must first measure where most of the activities of software vulnerability markets occur.

Figure 11 shows that all the main activities of vulnerability markets (buying and selling) occur during the discovery phase and before the exploitation, disclosure, and patching phases.

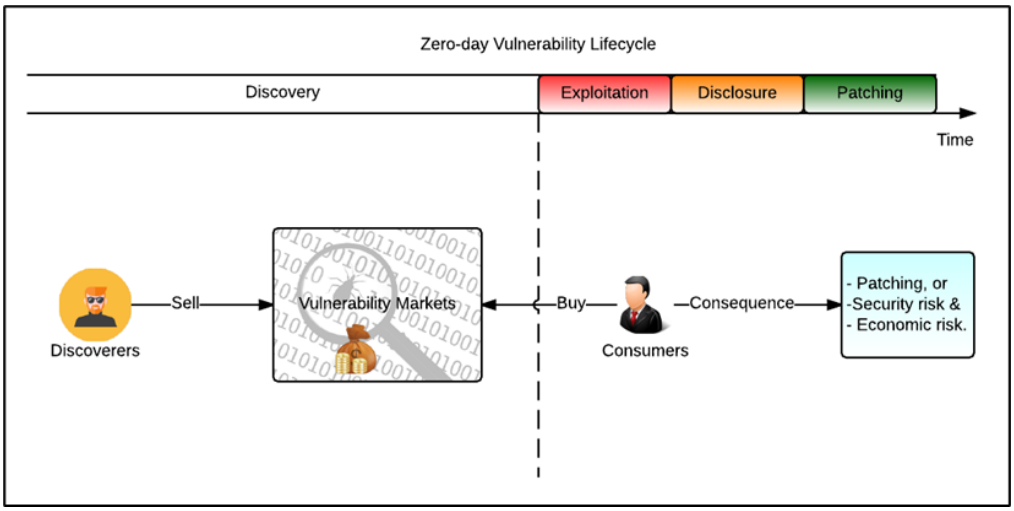

Figure 11. Economic model of the relationship between the vulnerability lifecycle and vulnerability markets.

For vulnerability buyers and sellers, the discovery phase provides a suitable environment that is separated from any factors that may affect the price negatively; this is important for any market looking to maintain continuous work. In addition, the markets must follow a cycle like a money cycle in many of the phases (discovery, exploitation, disclosure, and patching). This is directly related to the vulnerability lifecycle, especially the discovery phase. If the players of vulnerability markets (buyers and sellers) are not motivated, this will greatly affect the vulnerability lifecycle. For instance, if there is no monetary reward, which is the main motivation for discoverers, the discovery operations regarding vulnerability might decrease until the vulnerability lifecycle becomes slow and difficult. On the other hand, if the vulnerability markets are active in providing several rewards, the vulnerability lifecycle will be fast; this may lead to more risk if we do not try to manage the vulnerability markets and study their transactions. Thus, there is a directly proportional relationship between the vulnerability lifecycle and vulnerability markets.

4.2.3. Discovery Phase and Vulnerability Markets

Most of the buying and selling transactions occur during the discovery phase of the vulnerability lifecycle (Figure 11). This is logical considering that most of the vulnerabilities in the discovery phase have not yet been disclosed to the public or to specific individuals or organizations. Therefore, the vulnerabilities are considered a distinguished commodity that should be kept confidential and that are valuable in terms of the security risk from exploitation by the buyer, and the economic impact after the security risk occurs.

4.2.4. Exploitation Phase and Vulnerability Markets

If the software vendors or software system owners know that some of the vulnerabilities in their software or systems have been exploited by some consumers (individuals or organizations), the effect is minimal because everything has already been done, and there is no impact on the markets. However, the prices of vulnerabilities might decrease sharply. In contrast, other types of vulnerability markets, such as the black market, can

affect the exploitation phase. The risk measurement for monitoring black markets might prove to be a good evaluator of risk management and prioritization [33]. In addition, most vulnerabilities used during attacks or exploitation come from the black market.

4.2.5. Disclosure Phase and Vulnerability Markets

In this phase, there is a huge impact on the vulnerability price and demand since the vulnerability has been disclosed. We expect the prices to drop sharply near to zero because the vulnerability has been exploited by hackers. Usually, the software vendors or systems will fix the vulnerability as soon as a patch is ready and available.

4.2.6. Patch Management Phase and Vulnerability Markets

The patching phase is an important part of the vulnerability lifecycle because the patch release may protect the system by removing the vulnerability [28]. The timing of the patch is critical [34]. If the security patch is applied too early, system administrators could experience instability because of some vulnerabilities in the patches (low patch quality). If the patch is applied too late, attackers could exploit the vulnerability. Therefore, choosing the best time for patching is crucial and is typically 10 to 30 days after the discovery date, although a zero-day patch provides interesting insight into the security performance of vendors [35]. Timely patch release by software vendors for product vulnerabilities is one of the main factors in making products more secure. Sometimes using information on crowdfunding security, such as bug bounty programs, can have negative or positive effects based on the vulnerability reward amount that is provided by vendors, which can either encourage or delay discoverers' submitting their vulnerabilities [36]. Understanding the relationship between vulnerability disclosure impact on patch release decisions and the behavior of software vendors is essential to achieving a high degree of security since information security breaches, which occur when cyberattacks exploit vulnerabilities, are becoming a significant issue.

4.2.7. Vulnerability Prices during the Vulnerability Lifecycle

Here, we theoretically study vulnerability price movements during each vulnerability lifecycle phase for each main vulnerability market. A change in the vulnerability price indicates that there is a relation between the vulnerability lifecycle and vulnerability markets. However, we do not have actual data to compare. We expect that the vulnerability price increased, decreased, or remained stable. Of course, there are several factors that affect the price, such as the importance of the vulnerability and its impact when it is exploited. We define three related concepts to determine the vulnerability price: normal: expected price (or reward) range associated with selling or purchasing the vulnerability in a certain vulnerability market; increment: the vulnerability price probably increases above the normal price of the vulnerability; and decrement: the vulnerability price probably decreases below the expected normal price of the vulnerability.

We can use the average vulnerability reward as the vulnerability price for each severity level (low, medium, etc.), but we cannot apply it here as other vulnerability markets are included, not just regulated markets. Also, we can use the average cost to fix the vulnerability price, but again, we cannot apply it because data are generally not available.

Table 3 shows the vulnerability price in different vulnerability markets depending on the vulnerability lifecycle phase. There is a strong relationship between vulnerability markets and the vulnerability lifecycle. Therefore, the price range of vulnerabilities in the discovery phase remains unchanged in regulated markets because the rewards range is fixed depending on some criteria; the price range may change negatively in online forums where money is not generally important, or positively in gray and black markets where the price depends on bidding, or by a huge amount observed when a vulnerability is exploited.

However, we expected the vulnerability price to decrease in all the types of vulnerability markets, because vulnerability is becoming more recognized by researchers who work in the field.

Table 3. Vulnerability price (increment ++, normal +-, or decrement –) during the vulnerability lifecycle phases.

Market Type	Discovery	Exploitation	Disclosure	Patching
Regulated	+-	–	–	–
Online Forums	–	–	–	–
Gray (Brokers)	++	–	–	–
Black	++	–	–	–

4.2.8. Relationship between the Vulnerability Discovery Rate and Vulnerability Rewards

In this section, we examine whether there is a relationship between the vulnerability discovery rate and the number of vulnerabilities that were rewarded by Firefox and Chrome rewards programs. This will be proven by determining if there is a relation (connection) between the number of vulnerability rewards and the discovery rate each year.

We classified the discovery rate and the number of vulnerability rewards presented to Firefox and Chrome vulnerabilities into low, medium, high, critical, and unknown security impacts. We then used the Pearson linear correlation coefficient (r) to measure the dependency between the discovery rate and number of vulnerability rewards in the same year for each severity impact category. We found that there is a high positive correlation for Firefox and Chrome (0.839 and 0.939, respectively). This indicates that increasing the number of vulnerability rewards results in a rise in the vulnerability discovery rate. This means that rewards (vulnerability market) have a big influence on the discovery phase (vulnerability lifecycle). Without rewards, movements in the vulnerability lifecycle could be hugely and negatively affected. This means that there is a relationship between the discovery rate and the number of vulnerability rewards. Therefore, when the researcher notes that most of the reported vulnerabilities that were rewarded have a high and critical impact severity, he will discover more vulnerabilities and report them in the appropriate vulnerability markets. Figures 12 and 13 illustrate the strong connection between the vulnerability rewards and the vulnerability discovery rate for Firefox and Chrome.

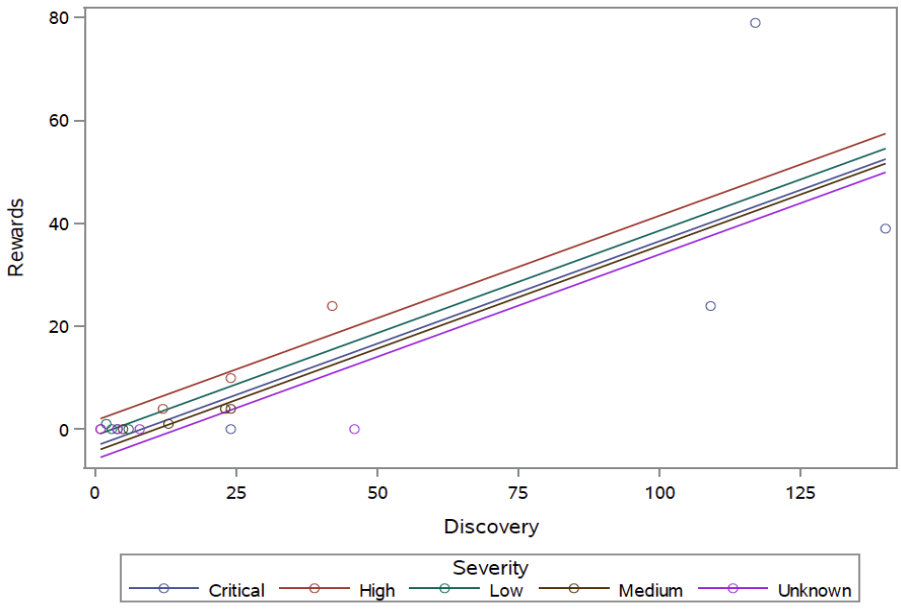

Figure 12. Analysis of covariance for Firefox vulnerability rewards.

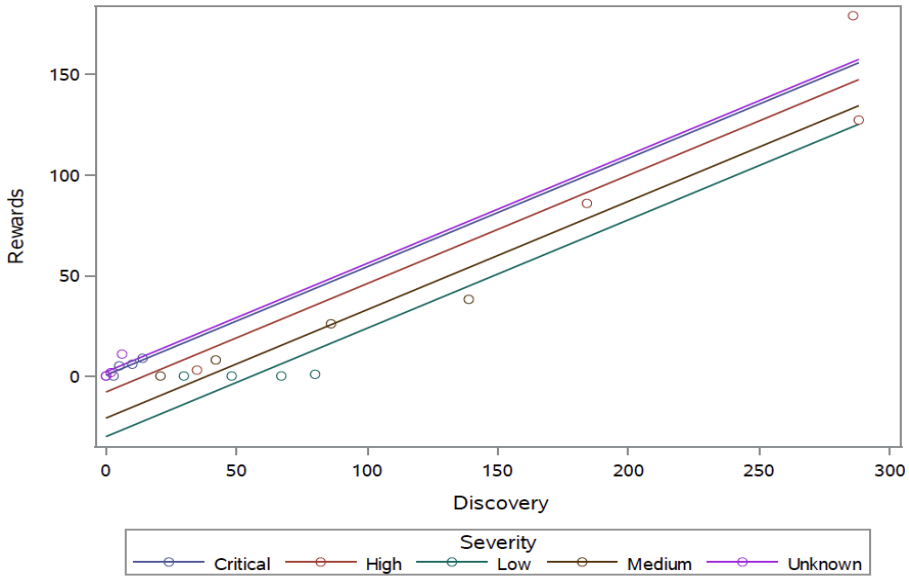

Figure 13. Analysis of covariance for Chrome vulnerability rewards.

4.3. Impact of the Vulnerability Lifecycle and Vulnerability Markets (RQ3)

The possible impact of the relationship between the vulnerability lifecycle and vulnerability markets is mostly risky in the case that the vulnerability markets are active or inactive. For example, if the markets are active, the risk will increase because money is the most important factor. Therefore, every discoverer will try to sell his/her vulnerabilities to buyers (consumers) depending on his/her way of thinking, behavior, manners, and motivation. The buyers will, in most cases, probably patch the vulnerability. On the other hand, discoverers and buyers whose main interest is not money, such as hacktivists, will find many vulnerabilities that can be used to harm other organizations or society.

Therefore, vulnerability markets should be active as it is impossible to find any software or a system that does not have a defect or vulnerability. The movement of these markets will push those responsible for security to develop their techniques to make software and systems more secure. Thus, further studies must be conducted on vulnerability markets and organizations to reduce the security risks.

Table 4 shows the security and economic risk impact for a vulnerability during its lifecycle using some main items of vulnerability markets, which include vulnerability market types, producers (discoverers), and consumers (buyers) [9]. The huge risk impact comes during the discovery phase for all the items. The phases of exploitation and disclosure oscillate between having high risks and no impact. After high-quality patching, no risk is expected. The risk model of vulnerability markets and the vulnerability lifecycle is demonstrated in Figure 14.

Table 4. A vulnerability risk assessment based on some vulnerability market factors (items) during the vulnerability lifecycle (H = high, M = medium, N = no impact).

Main Factors		Discovery	Exploitation	Disclosure	Patching
Discoverers:	Freelancer	H	N	N	N
	Captive	N	N	N	N
Markets:	Regulated	M	N	N	N
	Online forums	H	N	N	N
	Gray	H	N	N	N
	Black	H	N	N	N
Buyers:	Software Developers	N	N	N	N
	Hacktivists	H	H	H	N
	Government Agencies	H	H	H	N
	Malicious Attackers	H	H	H	N

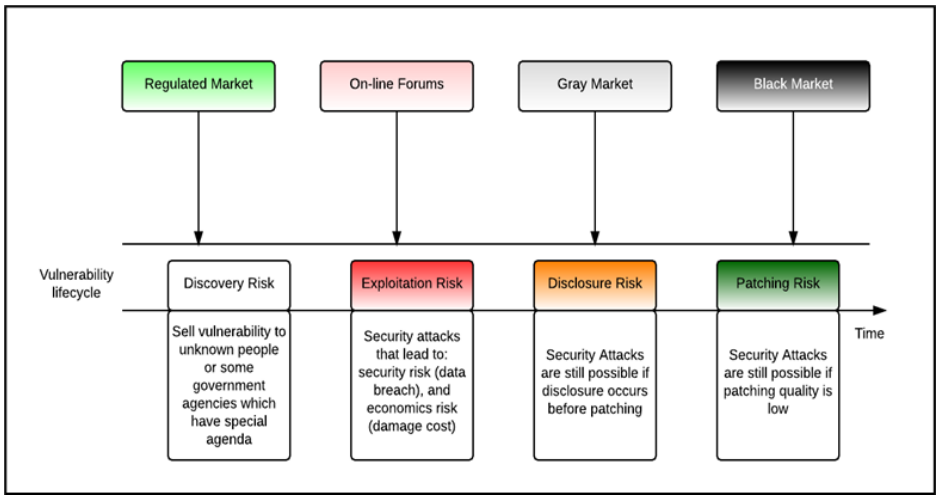

Figure 14. Risk model of vulnerability markets and the vulnerability lifecycle.

4.3.1. Vulnerability Security Risk

The chances of losing information and records have increased with the rise in most people's personal information being collected, stored, and transmitted by businesses in electronic form. Malicious hacking can exploit software vulnerabilities in data breach incidents and inflict harm on people or organizations by releasing personal data, which can result in harassment, embarrassment, impersonation, or theft.

4.3.2. Vulnerability Economic Risk

Several government agencies from different countries have begun investing in offensive and defensive capabilities for cyber warfare and espionage in the past few years [37]. Cyber capabilities have the potential to be far more cost-effective than traditional military weapons. According to reports, some vulnerabilities, as well as their exploits, can be worth a lot of money. This could result in a huge market change, and software developers may become more aggressive in terms of their rewards programs as a result.

After considering the risks and costs of losing information by exploiting software vulnerabilities from different marketplaces and breaches, the vulnerability rewards programs (VRPs) approach is a unique solution for making legitimate markets a safe and reliable place for selling and buying vulnerabilities.

5. Discussion and Open Problems

After analyzing the dataset and examining the relationship between vulnerability markets and the vulnerability lifecycles, we will now discuss the results, followed by some recommendations for reducing the security and economic risks as much as possible.

5.1. General Discussion

After investigating the connection between the vulnerability lifecycle and vulnerability markets, we found that all the activities of such markets occur during the discovery phase of vulnerability markets. Thus, the discovery phase has been identified as a very important phase that needs further consideration. In addition, there is a strong correlation between and impact resulting from vulnerability markets and the vulnerability lifecycle and security risk. This outcome is demonstrated by studying the relationship between the discovery rate and vulnerability rewards for the current data.

5.2. Open Problems for Vulnerability Markets and the Vulnerability Lifecycle

Focusing more on the vulnerability lifecycle will increase the understanding of how a vulnerability is created, how it works, and how such a vulnerability affects the lives of users and organizations. One suggestion involves focusing on current software (source

codes) or system structures by using penetration tests, for example, and by providing very restrictive security rules and applying strong security programs to protect the end users. It is important to investigate all the phases of the vulnerability, and they should be linked to the potential losses and costs for all layers of society [38].

Black markets are an independent science. Therefore, all topics related to black markets should be analyzed. For instance, we need to understand the psychology of the bidders and their strategies. This may help us to understand their thinking styles and how unregulated markets (black markets) work.

A remediation strategy is necessary for black markets. Such a strategy can reduce or remove the impact of selling a vulnerability to malicious people or organizations. Implementing different strategies from other areas like business could help to solve issues in the area of vulnerability software.

The behavior of software vendors regarding quick patch releases depends on several factors, such as the disclosure of the vulnerability. The early release of a patch is good for the product, but not for the patch quality.

Exploitation activities are a more interesting index of risk than the number of vulnerabilities since hackers are sophisticated and economically driven [33]. Thus, black market economics can lead to focusing on attacking processes and future trends; additionally, it can be useful for better assessing security and rethinking the priorities of patches and patching behavior.

5.3. Open Problems for Security and the Economic Impact

The cost of information loss is not small, and it increases yearly. Therefore, there is a need for a good economic strategy for software products. Regarding this point, the approach of rewards programs will contribute to protecting these products and reducing the risk to a minimum. This is one solution, but we need other ideas to solve the issues in this area, and some that need more investigation and discussion are as follows:

The risks and costs related to information loss are very high. More studies of the economic risks will encourage software vendors to invest in security and create incentives for the security community to protect their software systems.

Usually, vulnerability discoverers have the choice of either turning to black markets or other legitimate markets. We should encourage discoverers to choose the legitimate market option rather than black markets; this is because, despite the latter offering higher profits than legitimate markets, they mean that discoverers have to deal with malicious characters who cause harm to end users around the world.

Offering monetary rewards and increasing the size of the prized already offered can be used to attract discoverers to participate in legitimate markets instead of the black market, but there are other factors at play. Surveying discoverers could help to reveal these.

The black market is not a regulated market. Therefore, we also need more studies about the possibility of eliminating or managing these kinds of markets.

5.4. Threat to Validity

We collected reported vulnerabilities for both browsers during the specified period (2009 to 2012). Unfortunately, we did not use more additional data, since we did not know which reported vulnerabilities (CVE-ID) were rewarded or the amount of the rewards. We attempted to contact the security teams of those browsers and some experts who work at Mozilla and Google to obtain the missing data; unfortunately, we did not receive a response from them.

We expected the dataset to contain all the monetary transactions (rewards) performed between reporters and the Firefox and Chrome security teams. Thus, in reality, we focused on regulated markets. We could not study the other markets' transactions because the data are not publicly available or are insufficient for analysis.

6. Conclusions and Future Work

To investigate the research questions, we analyzed the dataset to determine vulnerability market types. The fact that money is the main motivating factor that drives vulnerability markets and that these markets are impacted by the vulnerability lifecycle is logical, but no research proof exists yet. Therefore, studying these markets with actual data and examining the relationship between vulnerability markets and the vulnerability lifecycle, theoretically, and statistically, is considered to be strong evidence that the vulnerability lifecycle depends on vulnerability markets.

As we know, some vulnerability markets (e.g., black markets) involve selling vulnerabilities to known or unknown people who pay a high price and have hidden agendas in terms of harming others. This leads to security data breaches, which produce many security and economic risks.

However, the future work will focus on creating a market model that encourages vulnerability discoverers to sell their discoveries to different and creative legitimate markets in which the buyers are software vendors instead of black marketers. Also, the development and verification of mathematical models will be implemented to simplify the existing comparisons and future analysis of the vulnerability lifecycle and vulnerability markets in the software industries. In addition, more studies on new and current datasets about other web browsers can lead to an analytical comparison with the datasets used in this study to monitor and follow the evolution in the relationship between the software vulnerability lifecycle and vulnerability markets over the last decade.

Funding: This research was funded by King Abdulaziz University under grant no. D-147-611-1440.

Acknowledgments: This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant no. D-147-611-1440. The author, therefore, gratefully acknowledge the DSR technical and financial support.

Conflicts of Interest: The author declares no conflict of interest.

References

1. McGraw, G. *Software Security: Building Security*; Addison Wesley Professional: Boston, MA, USA, 2006.
2. Humayun, M.; Niazi, M.; Jhanjhi, N.Z.; Alshayeb, M.; Mahmood, S. Cyber security threats and vulnerabilities: A systematic mapping study. *Arab. J. Sci. Eng.* **2020**, *45*, 3171–3189. [CrossRef]
3. Algarni, A.M.; Malaiya, Y.K. A consolidated approach for estimation of data security breach costs. In Proceedings of the 2nd International Conference on Information Management (ICIM), London, UK, 7–8 May 2016; pp. 26–39.
4. Algarni, A.M.; Thayananthan, V.; Malaiya, Y.K. Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems. *Appl. Sci.* **2021**, *11*, 3678. [CrossRef]
5. Arnold, B.; Qu, Y. Detecting software security vulnerability during an agile development by testing the changes to the security posture of software systems. In Proceedings of the 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 16–18 December 2020; pp. 1743–1748.
6. Arora, A.; Telang, R.; Xu, H. Optimal policy for software vulnerability disclosure. *Manag. Sci.* **2008**, *54*, 642–656. [CrossRef]
7. Kuehn, A.; Mueller, M. Shifts in the cybersecurity paradigm: Zero-day exploits, discourse, and emerging institutions. In Proceedings of the 2014 New Security Paradigms Workshop, Victoria, BC, Canada, 15–18 September 2014; pp. 63–68.
8. Frei, S.; Schatzmann, D.; Plattner, B.; Trammell, B. Modeling the security ecosystem-the dynamics of (in) security. In *Economics of Information Security and Privacy*; Moore, T., Pym, D., Ioannidis, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; pp. 79–106.
9. Algarni, A.; Malaiya, Y. Software vulnerability markets: Discoverers and buyers. *Int. J. Comput. Inf. Sci. Eng.* **2014**, *8*, 71–81.
10. Algarni, A.M.; Malaiya, Y.K. Most successful vulnerability discoverers: Motivation and methods. In Proceedings of the 2013 International Conference on Security and Management (SAM), Washington, DC, USA, 2–6 September 2013; p. 1.
11. Fryer, H.; Simperl, E. Web science challenges in researching bug bounties. In Proceedings of the ACM Web Science Conference, New York, NY, USA, 25–28 June 2017; pp. 273–277.
12. Zhou, J.; Hui, K. Bug bounty programs, security investment and law enforcement: A security game perspective. In Proceedings of the 2019 Workshop on the Economics of Information Security (WEIS), Boston, MA, USA, 3–4 June 2019.
13. Li, Z.; Liao, Q. Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. *Gov. Inf. Q.* **2018**, *35*, 151–160. [CrossRef]
14. Li, Z.; Liao, Q. An economic alternative to improve cybersecurity of e-government and smart cities. In Proceedings of the 17th International Digital Government Research Conference on Digital Government Research, Shanghai, China, 8–10 January 2016; pp. 455–464.

15. Walshe, T.; Simpson, A. An empirical study of bug bounty programs. In Proceedings of the 2020 IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF), London, ON, Canada, 18 February 2020; pp. 35–44.
16. Ruohonen, J.; Allodi, L. A bug bounty perspective on the disclosure of web vulnerabilities. In Proceedings of the 17th Annual Workshop on the Economics of Information Security, Innsbruck, Austria, 18–19 June 2018.
17. Arora, A.; Telang, R. Economics of software vulnerability disclosure. *IEEE Secur. Priv.* **2005**, *3*, 20–25. [CrossRef]
18. Kesan, J.P.; Hayes, C.M. Bugs in the market: Creating a legitimate, transparent, and vendor-focused market for software vulnerabilities. *Ariz. Law Rev.* **2016**, *58*, 753–830. [CrossRef]
19. Ransbotham, S.; Mitra, S.; Ramsey, J. Are markets for vulnerabilities effective? *Mis Q.* **2012**, *36*, 43–64. [CrossRef]
20. Munaiah, N.; Meneely, A. Vulnerability severity scoring and bounties: Why the disconnect? In Proceedings of the 2nd International Workshop on Software Analytics, Seattle, WA, USA, 13 November 2016; pp. 8–14.
21. Burkart, P.; McCourt, T. The international political economy of the hack: A closer look at markets for cybersecurity software. *Pop. Commun.* **2017**, *15*, 37–54. [CrossRef]
22. Allodi, L. Economic factors of vulnerability trade and exploitation. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Dallas, Texas USA, 30 October–3 November 2017; pp. 1483–1499.
23. Arora, A.; Forman, C.; Nandkumar, A.; Telang, R. Competition and patching of security vulnerabilities: An empirical analysis. *Inf. Econ. Policy* **2010**, *22*, 164–177. [CrossRef]
24. Anderson, R.; Böhme, R.; Clayton, R.; Moor, T. Security economics and European policy. In *ISSE 2008 Securing Electronic Business Processes*; Pohlmann, N., Reimer, H., Schneider, W., Eds.; Springer: Berlin/Heidelberg, Germany, 9 October 2008; pp. 57–76.
25. Moore, T. The economics of cybersecurity: Principles and policy options. *Int. J. Crit. Infrastruct. Prot.* **2010**, *3*, 103–117. [CrossRef]
26. Telang, R.; Wattal, S. An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Trans. Softw. Eng.* **2007**, *33*, 544–557. [CrossRef]
27. Arbaugh, W.A.; Fithen, W.L.; McHugh, J. Windows of vulnerability: A case study analysis. *Computer* **2000**, *33*, 52–59.
28. Marconato, G.V.; Kaâniche, M.; Nicomette, V. A vulnerability life cycle-based security modeling and evaluation approach. *Comput. J.* **2013**, *56*, 422–439. [CrossRef]
29. Shahzad, M.; Shafiq, M.Z.; Liu, A.X. A large scale exploratory analysis of software vulnerability life cycles. In Proceedings of the 34th International Conference on Software Engineering (ICSE), Zurich, Switzerland, 2–9 June 2012; pp. 771–781.
30. Frei, S.; May, M.; Fiedler, U.; Plattner, B. Large-scale vulnerability analysis. In Proceedings of the 2006 SIGCOMM Workshop on Large-Scale Attack Defense, New York, NY, USA, 11–15 September 2006; pp. 131–138.
31. Yue, W.T.; Wang, Q.; Hui, K. See no evil, hear no evil? Dissecting the impact of online hacker forums. *Mis Q.* **2019**, *43*, 73–95. [CrossRef]
32. Finifter, M.; Akhawe, D.; Wagner, D. An empirical study of vulnerability rewards programs. In Proceedings of the 22nd USENIX Security Symposium, Washington, DC, USA, 14–16 August 2013; pp. 273–288.
33. Allodi, L. The dark side of vulnerability exploitation: A proposal for a research analysis. In Proceedings of the ESSoS Doctoral Symposium, Eindhoven, The Netherlands, 15 February 2012.
34. Beattie, S.; Arnold, S.; Cowan, C.; Wagle, P.; Wright, C.; Shostack, A. Timing the application of security patches for optimal uptime. In Proceedings of the LISA '02: Sixteenth Systems Administration Conference, Philadelphia, PA, USA, 3–8 November 2002; Volume 2, pp. 233–242.
35. Frei, S.; Tellenbach, B.; Plattner, B. 0-day patch exposing vendors (in) security performance. In Proceedings of the BlackHat Europe, London, UK, 3–6 December 2008.
36. Mingyu, G.; Yang, Y.; Babar, M.A. Cost sharing security information with minimal release delay. In Proceedings of the International Conference on Principles and Practice of Multi-Agent Systems, Tokyo, Japan, 29 October–2 November 2018; pp. 177–193.
37. Greenberg, A. Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits, Forbes. Available online: http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/ (accessed on 25 July 2022).
38. Mann, C.L. Information Lost (Apologies to Milton). In *Economics of Digitization*; Goldfarb, A., Tucker, C., Greenstein, S., Eds.; University of Chicago Press: Chicago, IL, USA, 2013.