Synthesis

Autor / Date	Topic / Focus / Questions	Concept/ Theoretical model	Paradigm / Method	Context / Setting / Example	Findings	Limitations / Gaps (Future Research)
Radianti, J., & Gonzalez, J. J. (2007, July).	"*This work is a preliminary model to build a structure that may explain the factors influencing the emergence of vulnerability black market and to simulate undesired consequences from desired effect to eliminate software vulnerabilities "pg1* This work tries to establish what factors effect the emergence and growth of the black-market vulnerabilities.	preliminary system dynamics model	**Quantitative Data** **Simulation**	These models were based off a simulation that consisted of four main assumptions for the behavior of the system over time in the market. These four systems were the base run, full disclosure, a legal market, and lastly a risky environment.	There are some loops that counteract the effects of the intended policy. Zero-day exploits, rush patch cycle as well as supply and demand on vulnerabilities because of the disclosure policy. The vulnerability black market may not grow as fast as what is expected Or might be contained if the legal system effectively can create a situation where hackers will have higher risk of	• Empirical data and evidence • explore some policy levers relevant for our case – *responsible disclosure* • plan to simulate some policies that are pertinent to the software quality improvement and the vulnerability black market issue

					conducting cybercrime.	
Algarni, A. M., & Malaiya, Y. K. (2014).	"…major percentage of discoverers... are unaffiliated with the software developers and thus are free to disseminate the vulnerabilities they discover in any way they like. As a result, multiple vulnerability markets have emerged. In some of these markets, the exchange is regulated, but in others, there is little or no regulation " p1 this article goes in depth into the actual vulnerability market, both the regulated and unregulated, to gain a better concept of where and why this information is being sold.	the most prolific vulnerabilities over the past decade to understand the motivation, methods, and the overall risk it has on society today *top vulnerability discoverers' answers to specific questions about their vulnerability discovering and reward programs*	Quantitative Data Analysis on real life hackers with motivating factors, stop discovering, impact of rewards program, and applying to rewards program	the top vulnerability's discoverers on OSVDB in the last decade	The result of this work shows that majority of the vulnerabilities found are outside of the software developers' company, and the motivation behind these attacks are mostly due to money rewards. Regulated markets such as reward programs, the software vulnerabilities are disclosed in a proper and responsible way compared to the unregulated markets.	• There is a need to collect data about the transactions in the regulated and the unregulated markets so that the processes can be modeled accurately • With a dynamically changing field, studies such as this need to be repeated to see if there are any observable trends in terms of the vulnerabilities that end up in the legitimate and black market periodically, and the subsequent risks to society.

Algarni, A. M. (2022).	this article investigates the vulnerability regulated markets of Chrome and Firefox. As well as the correlation between vulnerability markets and the vulnerability lifecycle, and how these contributions may put people and companies at a security and economic risk "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	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).	Quantitative Data The type of vulnerability market to which the reporter might belong depending on the availability and reliability-captive market, vulnerability rewards program, security service companies, and publicity.	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	The findings form the article state that there is a strong correlation between the vulnerability lifecycle depending on the vulnerability markets Studying these markets with actual data and examining the relationship between vulnerability markets and the vulnerability lifecycle, theoretically, and statistically, is strong evidence that the vulnerability lifecycle depends on vulnerability markets.	• 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 • 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

	statistical approaches. Furthermore, we discussed the potential risks for people and organizations in terms of security and economics" p1					vulnerability lifecycle and vulnerability markets over the last decade.
L. Allodi, W. Shim and F. Massacci (2013)	quantitative assessment of the risks coming from the illegal market. As well as reducing overall attacks against users and companies. " In this paper, we focus on making a quantitative assessment of the risk of attacks coming from such markets, and investigating the expected reduction in overall attacks against final users if, for example, vulnerabilities traded in the black markets were all to be promptly patched" p1	EU-IST-NOE-NESSOS and EU-SEC-CP-SECONOMICS and TENACE PRIN Project (n. 20103P34XC) founded by the Italian Ministry of Education, University and Research. Symantec's attack data sharing platform WINE.	Quantitative Data Methods used in this article range from the WINE-DB, EKITS, NVD, and CVSS score.	Retrieve the data in EKITS directly from various black markets. WINE-DB is our ground truth dataset. It is a composition of publicly available data on attacked CVEs (SYM) and real attack data as collected by Symantec sensors worldwide and shared with researchers through the WINE data sharing program	Volumes of attacks coming from vulnerabilities in the black markets. Black markets monitoring results as a, on average, 20% more effective strategy than those currently enforced.	• It must be noted that this analysis of the volumes of attacks from the black market, is *not* by itself evidence of the importance of the actual exploits and tools traded in the black markets. • We do not have any proof that the actual attacks recorded in the WINE-DB dataset are delivered by means of exploit kits.

A. A. Younis and Y. K. Malaiya (2014)	A new metric that can be used for earlier detection and as an indicator, as well as a developed model that uses machine learning to predict rather a vulnerability is likely to be exploited or not. " we propose using the suggested metric as feature to construct a model using machine learning techniques for automatically predicting the risk of vulnerability exploitation" p1	construct a model based on machine learning techniques that uses the proposed metric as feature to predict the risk of vulnerability exploitation.	Quantitative Data Support Vector Machines (SVMs).	Are based off the research models of using measurement-based approaches, model-based approaches, test-based approaches, and analysis-based approaches.	Proposed a new metric that can be used as an earlier indictor of vulnerability exploitation based on software structure properties. Propose to develop a model that uses machine learning techniques to predict whether a given vulnerability is likely to be exploitable or not. The developed model can help decision makers prioritize their actions objectively based on function structure features.	• measure the effectiveness of our model • performance of the proposed predictive model, we will evaluate the accuracy, the area under the receiver operating characteristics curve (AUC), and false positive rate (FPR) as measures.
J. Radianti, E. Rich and J. J. Gonzalez (2009)	"Simulations find that if legal markets expose vulnerabilities that go unresolved, the security and quality of software may suffer more than in the absence of a legal	dynamic simulation models	Quantitative Data Simulation - concept model captures an abstract example of	The first scenario (Current) represents the absence of a legal market for overtly compensating hackers for their work.	Find that there is a possibility of these markets existing to help and create these security and media companies due to the lifecycle	• Much of the transaction detail is hidden in the privacy of personal messaging • participants in these black

	market. Thus, the problem scope expands beyond vulnerability trading to one that requires active participation and reaction by software vendors." Introduce a simulation model that produces how vulnerability discoveries possibly can be placed in a duel legal black-market concept		parallel legal and illicit markets.	A second scenario (Legal Market) assumes activation of the legal market. A third scenario (Manifest) represents manifested through attacks or extortion threats. The others through reports to vendors, or postings on web sites, presumably with more information about how the problem was identified. A fourth scenario (Consumer) in which is referencing the consumer exposure to these vulnerabilities in these markets.	and behaviors of the vulnerabilities Find that illicit markets end up producing an increase in our software quality and accelerated patching along with the speed of which we must do this. The process by which transitions from black to white markets develop and the resultant effects on overall software quality Vulnerability discovery is accelerated, it also becomes necessary to speed the development of patches for these flaws. If this is lacking, more manifest vulnerabilities	markets can be turned to serve more conventional needs while not adding risks to the environment • Such counter-intuitive results argue for careful examination of the context and grounding for implementing legal markets as a counter for vulnerability black markets.

					remain, which in turn may increase the exposure of customers and vendors	
Algarni, A. M. (2016).	" Assessing the impact of data breaches will allow organizations to assess the risks due to potential breaches and to determine the optimal level of resources and effort needed for achieving target levels of security. " p1 To build a stronger approach for identifying key factors contributing to the breach cost as well as assessing the impact of these breaches to allow for the correct resources, time, and efforts it takes in achieving the required security level you or your company desire.	Computational model for estimating the costs and probabilities of data breaches for a given organization. The model of data breach cost per record and the probability will use the method of "multiplicative model"	Quanatative Data Method of "multiplicative model" similar to the other quantitative models such as the defect density model , and software cost estimation model	Have identified the most prolific vulnerability discoverers throughout the past decade and examined their motivation and methods Actual data representation of the significant factors minus the redundant factors to merge a quantitative model of data breach costs and probability	This model can scale an economical proportional data breach probability, that is able to properly allow for optimal investments and implementations to increase your security The potential cost of information loss to businesses and society is increasing yearly	• Continue to investigate and study the reasons that make the vulnerability markets are not fully organized, which result in risks that harm economies or societies. • we need to create new vulnerability markets that are suitable for the different types of vulnerability discoverers • markets should be legitimate, attractive, and easy to deal with so they are a good income source for both sellers and buyers

						• studying the rewards buyers give to sellers should be reasonable, depending on supply and demand and other commercial market concepts. • work needs for further examination of the markets in more detail – transactions in legal and illegal markets • dynamically changing field, studies such as this need to be repeated to see if there are any observable trends in terms of the vulnerabilities that end up in the legitimate and

						black market periodically
Radianti, J., & Gonzalez, J. J. (2007, January)	This study aims to see exactly if the legal market helps reduce the trading of vulnerabilities on the black market "Whether the attempt to legalize the vulnerability market helps to reduce the vulnerability information circulating in the black market"	System dynamics model showing the growth of the vulnerability black market A simple conceptual model is developed and some simulations using the model are implemented to learn whether the attempt to legalize the vulnerability market helps to reduce the vulnerability information circulating in the black market	Quantitative Data Simulation	Simulation software Vensim Three what ifs' • What happens if communication and technology available today allow the criminals and hackers to share information and share experience about unknown vulnerabilities and successful attacks? • What occurs if vendors can develop patches faster to constrain the criminals' opportunities to exploit unknown malicious code?	The expansion of a black market for software vulnerabilities might significantly increase the risk of unplanned downtime from unknown vulnerability exploits. By having a legitimate market to which these vulnerabilities can be properly disclosed and by having a financial reward there is a shrink in the black market. Incentives to sell vulnerability findings to vendor shrink the vulnerability trading in the black market.	• The problems with such solution are the speed of all 'other parties' to find vulnerabilities as compared with the speed of the hackers • The hackers might sell the information to both parties: vendors and criminals. Our model so far neglects this issue and only considers the options of selling vulnerabilities to the vendors or selling them to malicious agents. • the importance of considering the risk of unknown vulnerability attacks faced by the company

				• What happens if vendors establish a legal market as a countermove against the black market?	understanding this hidden threat should also be relevant for any company relying on computer networks for their primary business.	transitioning to Integrated Operations: Such risk might become an unexpected threat to their security