Mathematical Biosciences and Engineering

http://www.aimspress.com/journal/mbe

MBE, 20(11): 19012–19039.
DOI: 10.3934/mbe.2023841
Received: 31 July 2023
Revised: 11 September 2023
Accepted: 21 September 2023
Published: 10 October 2023

Research article

The impact of regulatory mechanisms on vulnerability disclosure behavior during crowdsourcing cybersecurity testing

Liurong Zhao*, Xiaoxi Yu and Xinyu Zhou

School of Economics and Management, Nanjing Tech University, Nanjing 211816, China

* **Correspondence:** Email: zhaoliurong@njtech.edu.cn.

Abstract: There are various regulatory mechanisms to coordinate vulnerability disclosure behaviors during crowdsourcing cybersecurity testing. However, in the case of unclear regulatory effectiveness, enterprises cannot obtain sufficient vulnerability information, third-party crowdsourcing cybersecurity testing platforms fail to provide trusted services, and the government lacks strong credibility. We have constructed a tripartite evolutionary game model to analyze the evolutionary process of the equilibrium of {legal disclosure, active operation, strict regulation}, and the paper reveals the impact of three regulatory mechanisms. We find that these participants' positive behaviors are in a stable state. Higher initial willingness accelerates the speed of reaching the evolutionary stability of the system, and this equilibrium is satisfied only if the governmental regulatory benefits are sufficiently high. Regarding the punishment mechanism, increased punishment for enterprises causes them to adopt positive behaviors faster, while the opposite occurs for platforms; increased punishment for platforms drives both participants to adopt positive behaviors faster. Concerning the subsidy mechanism, increased subsidy to enterprises causes them to adopt legal disclosure behaviors faster, while platforms remain unresponsive; increased subsidy to platforms motivates both players to choose their own positive behaviors. In terms of the collaborative disclosure mechanism, excessive collaborative costs reduce the platforms' willingness to operate actively, which decreases the enterprises' incentives to disclose vulnerability legally. These findings guide the government to establish suitable mechanisms to regulate the participants' behavior and promote the healthy development of the cybersecurity crowdsourcing industry.

Keywords: cybersecurity; vulnerability disclosure behavior; regulatory mechanism; third-party crowdsourcing cybersecurity testing platform; white-hat hackers; tripartite evolutionary game

1. Introduction

Vulnerability disclosure has become a vital means of responding to cybersecurity incidents around the world, enabling organizations to timely obtain the necessary vulnerability information and take proactive response measures [1]. These disclosure behaviors, which include discovering, reporting, validating, patching and releasing potential vulnerabilities, are of great significance in reducing the risks and losses from their cybersecurity measures. However, with the expansion of hacker attacks and diversification of attack methods, more and more organizations are choosing non-disclosure or irresponsible disclosure due to lack of capability, causing massive financial and reputational losses. In response to these challenges, they are inclined to be involved in crowdsourcing cybersecurity testing to improve their vulnerability disclosure capabilities [2].

Crowdsourcing cybersecurity testing is the presentation of vulnerability services in the form of "crowdsourcing" in the field of cybersecurity. In this process, enterprises first release security testing programs, and then a group of white-hat hackers use sophisticated security techniques to test various scenarios, ultimately identifying exploitable vulnerabilities in the software or hardware. This open and innovative model can effectively overcome the traditional limitations of security professionals' scale within the enterprise, allowing them to quickly respond to cybersecurity vulnerabilities, shorten vulnerability disclosure time and greatly improve the probability of vulnerability discovery [3]. But for most enterprises, conducting crowdsourcing cybersecurity testing independently is cost-prohibitive, and solely relying on in-house recruited white-hat hackers can make it difficult to uncover all vulnerabilities within the systems. Therefore, the collaborative model between enterprises and third-party crowdsourcing cybersecurity testing platforms (TPCCTPs) has rapidly developed.

In 2016, the USA's Department of Defense (DoD) cooperated with HackerOne in the 'Hack the Pentagon' program, which for the first time allowed white-hat hackers to test the security vulnerabilities of the DoD's publicly accessible websites [4]. Later, such platforms, designed to attract white-hat hackers for vulnerability testing tasks, gradually emerged. However, these platforms initially only provided a community-based platform for hackers to disclose their discoveries without explicit requirements for enterprises to pay for it. After these platforms released vulnerability information, if enterprises did not review these vulnerabilities within a specified time frame, the platforms would publicly disclose them, exposing companies to the risk of malicious exploitation from this behavior. Because of enterprises' growing emphasis on cybersecurity, TPCCTPs have gradually evolved into bilateral platforms. Since then, one aspect has involved the review of vulnerability information submitted to the platforms, with enterprises providing a specific bounty for accepted vulnerability reports from white-hat hackers [4]. On the other side, the platforms take on the responsibility to disclose vulnerabilities, safeguarding the security of enterprises' information systems. This greatly enhances hackers' motivation to engage in crowdsourcing cybersecurity testing, which serves to reduce the risk of enterprises leaking vulnerability information and improve the efficiency and effectiveness of vulnerability disclosure [5]. Today, TPCCTPs such as Synack, Bugcrowd, OpenBugBounty, SynAck, etc. have collaborated with many enterprises. Figure 1 shows the vulnerability disclosure process of TPCCTPs.

However, this process involves frequent interactions among multiple participants and various resources, leading to a series of real-world issues. First, the goals of participants of vulnerability disclosure are different, and a consensus on collaborative vulnerability disclosure has not yet been

reached. Second, since all participants seek to maximize their own interests, this may lead to conflicts of interest that affect their willingness to actively participate in collaborative vulnerability disclosure. Third, due to the timeliness of vulnerabilities and the convenience of online transactions, the concealment of participants' illegal behavior is high, greatly hindering the ability of the government to detect and punish such behaviors, which will cause cybersecurity risks to diffuse. To address the existing issues, the regulatory mechanisms in crowdsourcing cybersecurity testing are necessary.

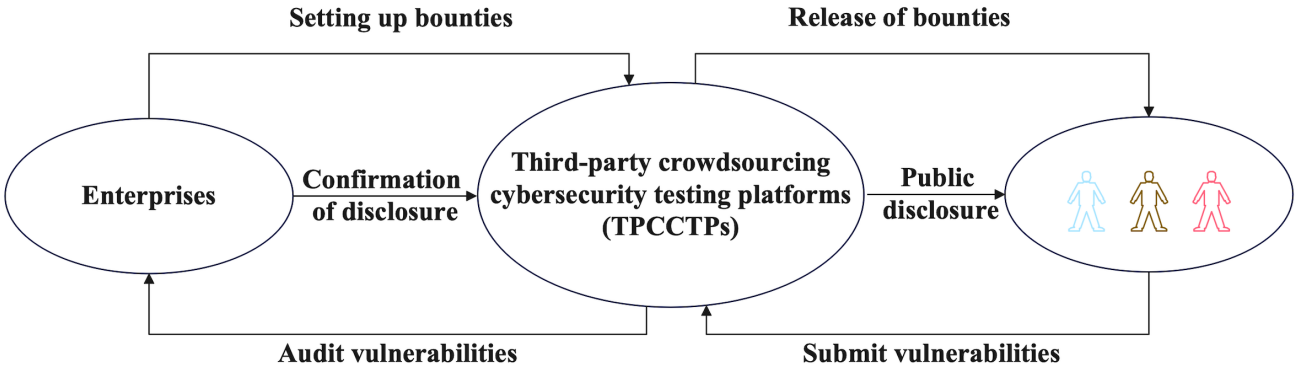


Figure 1. Vulnerability disclosure process of crowdsourcing cybersecurity testing.

Regulatory mechanisms refer to the set of processes, methods and standards through which authorities regulate the participants' behaviors [6]. Although many scholars have studied regulatory mechanisms, we have the following advantages over previous studies. First, from the theoretical perspective, it was mostly conducted in a legal field, but this study innovatively approaches the topic from a management perspective, studying the impact of regulatory mechanisms on participants' behaviors. Second, unlike previous studies that primarily focused on regulating white-hat hackers, this study considers the regulation of organizations such as enterprises and platforms, particularly exploring how to incentivize them to adopt positive vulnerability disclosure behaviors while balancing their interests. Third, previous studies on regulatory mechanisms for vulnerability disclosure were mostly investigated in a traditional context without considering the emerging service of crowdsourcing cybersecurity testing. It is necessary to explore whether and how traditional regulatory mechanisms adapt to the new issues. Specifically, we delve into scientific questions such as how the government adjusts its regulatory efforts and how to make policy adjustments based on the different responses of various participants to different mechanisms. Last but not least, previous studies mostly used theoretical frameworks to introduce vague and descriptive policy mechanisms, while this study employs game theory to investigate explicit and quantitative regulatory mechanisms, providing a more intuitive presentation of the characteristics and impacts of regulatory mechanisms.

Section 2 reviews the previous studies on vulnerability disclosure behavior and crowdsourcing cybersecurity testing, and it summarizes the research gaps. Section 3 analyzes the behavioral strategies of enterprises, TPCCTPs and the government, as well as their game theory-based relationship, summarizing the factors that impact their respective behaviors and presenting the corresponding tripartite evolutionary game model. Section 4 analyzes the stability results of the evolutionary game model in terms of the enterprises, TPCCTPs, government and system, respectively. Section 5 through numerical simulation, reveals the dynamic evolutionary law of the game among the

participants involved in crowdsourcing cybersecurity testing; it also explores the impact of three regulatory mechanisms on the evolutionary stable behavioral strategies. Section 6 provides the main conclusions, presents the limitations of the study and suggests perspectives for future research.

2. Literature review

2.1. Vulnerability disclosure behavior

Currently, academic research on vulnerability disclosure behavior focuses on four categories of topics: vulnerability disclosure behavioral antecedent, strategy, response and consequence. In terms of the behavioral antecedent, most scholars agreed that the incentives for white-hat hackers to disclose vulnerabilities are that they want to protect themselves and others from vulnerability exploitation [7] and enhance their own reputation and peer recognition [8], while enterprises aim to improve system security [9, 10]. Some also pointed out that the trust of enterprises in white-hat hackers is a prerequisite for vulnerability disclosure [11]. Providing transparent and accurate information to white-hat hackers helps to build trust relationships [12], which makes it possible to institutionalize the ethical hacker culture [13]. If enterprises perceive that white-hat hackers lack professional skills, produce low-quality vulnerability reports, have a high duplication rate of vulnerabilities or pose a risk of illegal system intrusion, this distrust will diminish the motivation for white-hat hackers to participate in vulnerability disclosure. In terms of behavioral strategy, the choice of vulnerability disclosure strategy is related to risk factors such as the severity of vulnerabilities, their scope of impact and the likelihood of exploitation [14]. When vulnerabilities are severe, stakeholders are more inclined to engage in responsible disclosure behavior and coordinated disclosure behavior [15]. When vulnerabilities have a wide scope of impact and a low likelihood of exploitation, stakeholders are more inclined to engage in non-disclosure behavior [16]. Only when the overall risk of vulnerabilities is low is full disclosure [17]. In terms of behavioral response, the response time of enterprises has been the focus of the research. Ahmed [18] found an inverse U-shaped relationship between the time to patch vulnerabilities and enterprises' experience in addressing such issues on crowdsourcing cybersecurity platforms. Jo [12] revealed that higher market concentration positively influences the time to patch vulnerabilities, while market position negatively affects the timeliness of patch releases. The vulnerability disclosure strategy increases the willingness of enterprises to develop patches [19] and shortens the time of patch release [9]. Furthermore, enterprises can be encouraged to release patches more swiftly by reducing the vulnerability protection period and embracing emerging technologies [20]. In terms of behavioral consequence, current research focuses on the impact of vulnerability disclosure on enterprise system security [21–23], stock market volatility [24, 25] and the effectiveness of vulnerability information dissemination [22]. There were some positive findings; for example, market-based vulnerability disclosure can effectively protect information systems because it encourages hackers to engage in legal transactions through a regulated market mechanism, reducing the risk of malicious exploitation of vulnerabilities [26]. On the other hand, the public disclosure of vulnerability information has a negative impact on enterprises' stock prices, which increases with longer response time [25]. Additionally, compared to responsible disclosure behavior and coordinated disclosure behavior, full disclosure behavior accelerates the spread of attacks. Especially when multiple vulnerabilities are disclosed simultaneously, hackers tend to attack specific vulnerabilities [22].

Current research on the regulation of vulnerability disclosure behavior is focused on two main topics: the legal boundary and legal risk. The legal boundary is a prerequisite for clarifying the legality of vulnerability disclosure behavior. Vulnerability disclosure exists in a legal gray area, where enterprises find it difficult to distinguish the intentions of hackers. Malicious hackers create risks by exploiting undiscovered vulnerabilities in applications, networks and services [21, 26]. Even ethical hackers, when reporting vulnerabilities, could be considered as having engaged in illegal behavior if they accessed or controlled software and hardware without authorization, and in the absence of following the prescribed procedure for vulnerability disclosure [8]. Legal risk is a key factor that hinders hackers' participation in vulnerability disclosure. Studies have shown that as many as 60% of white-hat hackers cite legal threats as a reason for not cooperating with enterprises to disclose vulnerabilities [6]. One can boost hackers' motivation by clarifying the rights and responsibilities in the vulnerability disclosure process, encouraging them to engage in vulnerability discovery activities without the risk of legal litigation. However, excessive restrictions or inconsistent legislation might result in a "chilling effect" on vulnerability disclosure, decreasing hackers' willingness to disclose vulnerabilities [27].

2.2. Crowdsourcing cybersecurity testing

Information technology is not absolutely secure, and there is always a risk of exploitation by malicious hackers. Especially emerging technologies like artificial intelligence and blockchain, which serve as means to protect enterprise information assets [28–31], have their own vulnerabilities that limit their widespread adoption. In recent years, with the popularity of crowdsourcing cybersecurity, bug bounty programs, vulnerability reward programs (VRPs), crowdsourced software testing and other crowdsourcing services have not only been able to detect traditional information technology vulnerabilities, but they have also become efficient in discovering vulnerabilities in emerging technologies, which has caused them to receive widespread attention.

Some scholars analyzed the positive impact of crowdsourcing cybersecurity testing on enterprises. These studies unanimously concluded that disclosing vulnerabilities based on crowdsourced cybersecurity platforms is effective for safeguarding cybersecurity [22, 32, 33]. Rewarding white-hat hackers who discover vulnerabilities, and thereby encouraging them to compete with malicious hackers, can reduce the risk of initial attacks and the frequency of vulnerability exploits [22, 32]. Pascariu [34] argued that crowdsourcing cybersecurity testing complements enterprises' security management, which enhances their brand image by obtaining vulnerable information through ethical hackers.

Some scholars have also studied white-hat hackers' characteristics on crowdsourcing cybersecurity testing platforms, such as their motivations and behavioral patterns [3, 35]. It has been demonstrated that money is a significant incentive for motivating white-hat hackers to disclose vulnerabilities [36–38]. Finifter et al. [39] conducted research on Google's VRP and Mozilla's Firefox VRP, revealing that variable rewards and incentive mechanisms are more attractive to white-hat hackers. Additionally, some hackers are driven by intrinsic motivation (i.e., enjoyment and a desire to learn) [40]. Other studies have also revealed heterogeneity among white-hat hackers, where factors such as increased social status, knowledge acquisition or altruism may motivate vulnerability disclosure behavior for different white-hat hackers [41]. Additionally, the mismatch between white-hat hackers' capabilities and the required vulnerability discovery skills decreases their

willingness to participate, which is in addition to the unclear rules and uncertain legal risks in the vulnerability disclosure process or on the crowdsourcing cybersecurity platforms. The incentives of crowdsourcing cybersecurity testing platforms to drive hackers' vulnerability disclosure behavior from a mechanism perspective have been a hotspot in recent years. Zhao et al. [5] evaluated different policies by developing an economic model, and they found that mechanisms incentivizing and encouraging security personnel are more effective. Luna et al. [38] investigated HackerOne's program rules, discovering a positive correlation between the comprehensiveness of crowdsourcing cybersecurity testing rules and the willingness of vulnerability disclosure behavior. Ahmed et al. [42] found that disclosing effective vulnerabilities attracts white-hat hackers, while repetitive and ineffective disclosure reports reduce the number of experienced hackers, so management mechanisms are crucial to attracting highly skilled ones. Additionally, some scholars have employed game theory to explore the impact of various mechanisms on participants' behavior in multi-agent interaction processes. Xiong et al. [43] constructed a game model with third-party vulnerability sharing platforms and found that establishing a credit system for patch development and improving the punishment mechanism for dishonesty contribute to security researchers' positive disclosure of vulnerabilities. Xu et al. [44] constructed a game model that confirmed that government punishment mechanisms can facilitate win-win situations for enterprises and consumers in certain scenarios.

In summary, existing research primarily focuses on the vulnerability disclosure behavioral antecedent, strategy, response and consequence of the single participant, as well as the legal boundary and risk faced by the hackers. It has been confirmed that crowdsourcing cybersecurity testing is an effective means to promote vulnerability disclosure behavior. Many scholars have also studied the impact of crowdsourcing cybersecurity testing on disclosure behavior from the perspectives of hacker characteristics and the mechanisms of the TPCCTPs. Although the motivations for white-hat hackers or enterprises are analyzed widely, the interaction among participants is rarely studied. Additionally, the influence of vulnerability attributes and enterprises' response time on vulnerability disclosure behavior has been emphasized, and the importance of legal factors as a tool to constrain white-hat hacker disclosure behavior has been underscored, but the policy's impact has been overlooked. Despite the in-depth investigations of previous studies on the impact of vulnerability disclosure behavior on enterprises' cybersecurity and stock market volatility, the social welfare or losses have not been considered. Furthermore, although it has been demonstrated that crowdsourcing cybersecurity platforms can promote enterprises' cybersecurity by incentivizing white-hat hackers to engage in vulnerability disclosure behavior, most studies have focused on platform reward mechanisms for hackers. Research on government incentives for enterprises and TPCCTPs is relatively limited, resulting in a lack of theoretical foundation for the healthy development of the cybersecurity crowdsourcing industry. Therefore, we have constructed an evolutionary game model that considers parameters such as punishments, subsidies, costs, social welfare, etc. We explore the regulatory mechanisms involving enterprises, TPCCTPs and the government, and analyze the mechanisms' impact on the vulnerability disclosure behavior of all participants. This study serves to provide theoretical support and practical recommendations that can be used by the government to regulate the vulnerability disclosure behavior of enterprises and TPCCTPs involved in crowdsourcing cybersecurity testing.

3. Construction of evolutionary game model

3.1. Problem description

Participants in crowdsourcing cybersecurity testing include enterprises, TPCCTPs, white-hat hackers and the government. However, it is important to note that white-hat hackers are fully managed by TPCCTPs, and they represent TPCCTPs' capability in vulnerability disclosure. Therefore, in this paper, we do not classify white-hat hackers as independent primary participants.

For enterprises, disclosing vulnerabilities typically involves vulnerability assessment, vulnerability risk evaluation, vulnerability remediation and vulnerability reporting. Due to constraints of vulnerability management capabilities, security awareness or the pursuit of profit maximization, enterprises may not necessarily adhere to prescribed procedures for vulnerability disclosure, and they may even engage in non-compliant concealment of vulnerabilities. Therefore, they have two behavioral strategies, i.e., "compliance disclosure" and "non-compliance disclosure".

For TPCCTPs, their vulnerability disclosure process includes organizing the vulnerability discovery, vulnerability submission, vulnerability assessment and notifying the enterprises to patch the vulnerabilities. Since enterprises and TPCCTPs are collaborators, and closer cooperation corresponds to more revenue for the TPCCTPs, they have no incentive to monitor whether the enterprise engages in compliant vulnerability disclosure behavior. However, with the gradual emergence of the trend of collaborative vulnerability disclosure, the government has begun to encourage TPCCTPs to actively cooperate with enterprises to establish channels for receiving and processing vulnerability information, which would assist enterprises in vulnerability assessment, remediation and reporting, to jointly maintain cybersecurity. Therefore, TPCCTPs have two behavioral strategies, i.e., "active operation" and "negative operation".

The government primarily refers to agencies responsible for cybersecurity regulation, including governmental departments from various countries, such as the National Security Agency of the USA, the National Cyber Security Centre of the UK and the Ministry of Industry and Information Technology of China, as well as cybersecurity technology centers such as the Computer Emergency Response Teams and Center for Internet Security. These agencies are responsible for managing vulnerability disclosure activities, and their responsibilities encompass coordinating the vulnerability disclosure process, promoting collaborative vulnerability disclosure and the real-time sharing of vulnerability information, jointly assessing and managing vulnerability risks and preventing illegal activities related to vulnerability disclosure. Theoretically, all enterprises' vulnerability disclosure behaviors should be regulated by the government. However, the practical situation indicates that vulnerability disclosure spans various industries with numerous enterprises of varying scales. Due to the constraints of limited human, financial and material resources, governmental regulatory efforts may vary significantly. Therefore, the government typically adopts two behavioral strategies, i.e., "strict regulation" and "lax regulation".

From the game process of the three participants, when enterprises choose non-compliance disclosure, they only acquire vulnerability information from TPCCTPs and do not follow the prescribed disclosure process. This leads to the failure to achieve the goal of collaborative vulnerability disclosure. In contrast, when enterprises choose compliance disclosure, TPCCTPs face the decision of whether to actively cooperate and assist the enterprise in improving the efficiency and quality of vulnerability disclosure. Additionally, TPCCTPs must decide whether to truthfully upload

feedback from white-hat hackers, vulnerability review reports and vulnerability information to a cybersecurity sharing platform. The government regulates the participants in crowdsourced cybersecurity testing based on relevant laws and regulations, including by imposing punishments and rewards on the TPCCTPs and enterprises to establish a collaborative vulnerability disclosure system. The game theory-based relationship between these three players is shown in Figure 2.

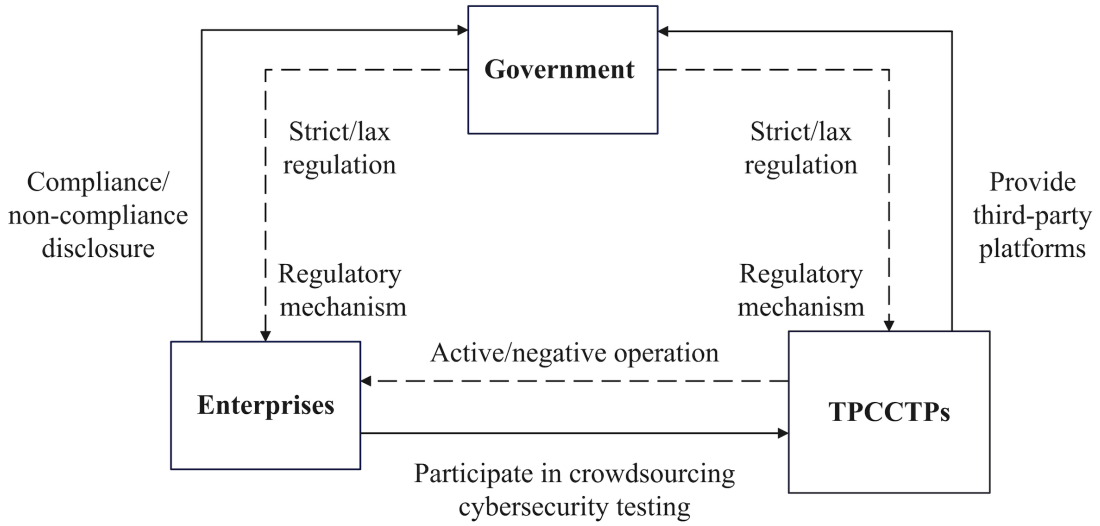


Figure 2. Game theory-based relationships among enterprises, TPCCTPs and the government.

3.2. Assumptions and parameters

Assumption 1. *The strategy set for enterprises is* {*compliance disclosure, non-compliance disclosure*}*; the probability of compliance disclosure is x, and the probability of non-compliance disclosure is* $1 - x$*. The strategy set for TPCCTPs is* {*active operation, negative operation*}*; the probability of active operation is y, and the probability of negative operation is* $1 - y$*. The strategy set for the government is* {*strict regulation, lax regulation*}*; the probability of strict regulation is z, and the probability of lax regulation is* $1 - z$*, where x, y and* $z \in [0, 1]$.

Assumption 2. *The basic benefits for enterprises participating in crowdsourcing cybersecurity testing are represented by* S_1*, and they include obtaining vulnerability information to improve system security, building user trust and establishing a positive credit of enterprises actively addressing security issues. The costs of compliance disclosure for enterprises are represented by* C_1*, and they include service fees for crowdsourcing cybersecurity testing services and the costs of complying with legal requirements for vulnerability repair, review and notification, which involve time, human resources and financial resources [45, 46]. When the government implements a regulation, enterprises' compliance disclosure behavior will garner them additional benefits, as denoted by* S_2*, and which include benefits obtained through channels for sharing vulnerability information and cooperative vulnerability risk mitigation. The costs of enterprises' non-compliance disclosure are represented by* C_2*, and they only include the service fees for crowdsourcing cybersecurity testing. In this case, enterprises may not disclose their adherence to the regulations, and may even opt for non-disclosure, so* $C_1 > C_2$*. There is no additional*

benefit from non-compliance disclosure.

Assumption 3. *The basic benefits of the TPCCTPs are denoted by P_1, and they are primarily composed of commissions paid by enterprises. The basic costs of TPCCTPs are denoted by C_3, and they include rule formulation, the recruitment of white-hat hackers, vulnerability assessment and review and communication with enterprises and white-hat hackers. When TPCCTPs adopt active operation behavior and enterprises choose compliance disclosure behavior, they collaborate in the area of vulnerability disclosure. At this time, TPCCTPs need to bear the collaborative costs of C_4, such as the costs of distributing and managing vulnerability information and coordinating vulnerability information reviews. This collaborative cost is influenced by the vulnerability testing cost. Specifically, when the vulnerability testing cost is too high, it may reduce TPCCTPs' willingness to participate in collaborative disclosure, leading to an increase in collaborative costs [47]. In addition, government regulation can bring the additional benefits of P_2 to the TPCCTPs, which increase as the TPCCTPs' disclosure capabilities grow. When TPCCTPs choose negative operation behavior, there are no additional benefits or collaborative costs.*

Assumption 4. *The costs of the government's strict regulation are denoted by C_5, and they include the costs of improving the establishment of a supervisory system for vulnerability disclosure, inspections of non-compliance with disclosure regulations, the optimization of cybersecurity vulnerability management technologies and participation in vulnerability disclosure reviews [1]. Strict regulation of the government can enhance public satisfaction and increase the government's credibility, thereby generating regulatory benefits, denoted by R. To guide enterprises and TPCCTPs toward positive behaviors, the government usually imposes punishments of K_1 and K_2 for non-compliance disclosure by enterprises and negative operation by platforms, respectively; these punishments include warnings, fines, production suspensions and rectifications. In the case of lax regulation, there are no regulatory costs or benefits.*

Assumption 5. *In the process of vulnerability disclosure, there are potential risks such as the leakage of vulnerability information and the spread of vulnerability exploitation [48]. When enterprises disclose compliance and TPCCTPs operate actively, the channels for vulnerability spread are usually preventable and controllable when the risk of vulnerability disclosure is not considered. When enterprises disclose non-compliance or TPCCTPs operate negatively, the responsible party must bear all of the losses, denoted by F. For example, if enterprises fail to timely patch vulnerabilities leading to their exploitation, or if TPCCTPs fail to effectively manage white-hat hackers resulting in the leakage of vulnerability information, the losses will be borne by the respective parties at fault. When both parties are at fault simultaneously, the coefficients of losses borne for enterprises and TPCCTPs are, respectively, d and $1 - d$, where $d \in [0, 1]$.*

Assumption 6. *Enterprises' compliance disclosure behavior is beneficial for maintaining public interests and reducing cybersecurity risks, thereby bringing societal benefits to the government. While TPCCTPs play a supportive role in this process and do not directly provide societal benefits, their active operation behavior contributes to maintaining cybersecurity. Nevertheless, TPCCTPs' negative operation behavior may lead to losses, and societal welfare M is only achieved when enterprises disclose compliance and TPCCTPs operate actively. In cases of lax regulation, the non-compliance disclosures of enterprises or negative operation of TPCCTPs may jeopardize public safety, resulting in societal losses, denoted by W.*

Table 1 presents the parameters along with their corresponding meanings.

Table 1. The main parameters of the tripartite regulatory game model for enterprises, TPCCTPs and the government.

Participants	Parameters	Meanings
Enterprises	S_1	The basic benefits of enterprises;
	S_2	The additional benefits of enterprises' compliance disclosure;
	C_1	The costs of enterprises' compliance disclosure;
	C_2	The costs of enterprises' non-compliance disclosure;
	F	The losses of enterprises' non-compliance disclosure;
	d	The coefficient of losses borne for enterprises;
TPCCTPs	P_1	The basic benefits of TPCCTPs;
	P_2	The additional benefits of TPCCTPs' active operation;
	C_3	The basic costs of TPCCTPs;
	C_4	The collaborative costs of TPCCTPs;
	F	The losses of TPCCTPs' negative operation;
	$1-d$	The coefficient of losses borne for TPCCTPs;
Government	R	The benefits of the government's strict regulation;
	C_5	The costs of the government's strict regulation;
	K_1	The government-imposed punishments for non-compliant disclosure by enterprises;
	K_2	The government punishments for negative operation by platforms;
	M	Social welfare under the conditions of enterprise compliance disclosure and platform active operation;
	W	Social loss under the conditions of enterprise non-compliance disclosure and platform negative operation

Based on the assumptions and parameters defined, the game payoff matrix of the tripartite was constructed as shown in Table 2.

Table 2. Payment matrix for the evolution game among enterprises, TPCCTPs and the government.

Strategies	Enterprises	TPCCTPs	Government
(x,y,z)	$S_1+S_2-C_1$	$P_1+P_2-C_3-C_4$	$R+M-C_5$
$(x,y,1-z)$	S_1-C_1	$P_1-C_3-C_4$	M
$(x,1-y,z)$	$S_1+S_2-C_1$	$P_1-C_3-K_2-F$	$R+K_2-C_5-W$
$(x,1-y,1-z)$	S_1-C_1	P_1-C_3-F	$-W$
$(1-x,y,z)$	$S_1-C_2-K_1-F$	$P_1+P_2-C_3$	$R+K_1-C_5-W$
$(1-x,y,1-z)$	S_1-C_2-F	P_1-C_3	$-W$
$(1-x,1-y,z)$	$S_1-C_2-K_1-dF$	$P_1-C_3-K_2-(1-d)F$	$R+K_1+K_2-C_5-W$
$(1-x,1-y,1-z)$	S_1-C_2-dF	$P_1-C_3-(1-d)F$	$-W$

4. Model analysis

4.1. Stability analysis of enterprises

According to Table 2, the expected income E_{11} or E_{12} of enterprises when they choose the "compliance disclosure" or "non-compliance disclosure" strategy are, respectively,

$$\begin{aligned} E_{11} = {} & yz\left(S_1 + S_2 - C_1\right) + y(1-z)\left(S_1 - C_1\right) + (1-y)z\left(S_1 + S_2 - C_1\right) \\ & + (1-y)(1-z)\left(S_1 - C_1\right) \end{aligned} \tag{4.1}$$

$$\begin{aligned} E_{12} = {} & yz\left(S_1 - C_2 - K_1 - F\right) + y(1-z)\left(S_1 - C_2 - F\right) + (1-y)z\left(S_1 - C_2 - K_1 - dF\right) \\ & + (1-y)(1-z)\left(S_1 - C_2 - dF\right) \end{aligned} \tag{4.2}$$

The average expected income $\overline{E_1}$ of enterprises is

$$\overline{E_1} = xE_{11} + (1-x)E_{12} \tag{4.3}$$

According to Formulas (4.1)–(4.3), we can further obtain the replicator dynamics equation for the behavior strategy selection of enterprises as follows:

$$F(x) = dx/dt = x\left(E_{11} - \overline{E_1}\right) = x(x-1)\left[C_1 - C_2 - Fd + (Fd - F)y - (K_1 + S_2)z\right] \tag{4.4}$$

The first-order derivatives of x and $G(y)$ are as follows:

$$\frac{d(F(x))}{dx} = (2x-1)\left[C_1 - C_2 - Fd + (Fd - F)y - (K_1 + S_2)z\right] \tag{4.5}$$

$$G(y) = C_1 - C_2 - Fd + (Fd - F)y - (K_1 + S_2)z \tag{4.6}$$

In order to find the probability of enterprises choosing compliance disclosure in the steady state, it must be satisfied that $F(x) = 0$ and $\frac{d(F(x))}{dx} < 0$. Because $\partial G(y)/\partial y < 0$, $G(y)$ is a decreasing function with respect to y.

When $y = \left[C_1 - C_2 - Fd - (K_1 + S_2)z\right]/(F - Fd) = y^*$, $G(y) = 0$, $\frac{d(F(x))}{dx} < 0$ and $F(x) = 0$, all values of x are in the evolutionary steady state at this time. When $y < y^*$, $G(y) > 0$ and $d(F(x))/\,dx|_{x=0} < 0$, $x = 0$ is the evolutionary stabilization strategy for enterprises. Otherwise, $x = 1$ is the evolutionary stabilization strategy. The phase diagram of the enterprise strategy evolution is shown in Figure 3.

Figure 3 shows that the probability that enterprises choose non-compliance disclosure behavior is V_{A_1} of A_1, and the probability that they choose compliance disclosure behavior is V_{A_2} of A_2:

$$V_{A_1} = \int_0^1 \int_0^1 \frac{C_1 - C_2 - Fd - (K_1 + S_2)z}{F - Fd} dzdx = \frac{2\left(C_1 - C_2 - Fd\right) - (K_1 + S_2)}{2(F - Fd)} \tag{4.7}$$

$$V_{A_2} = 1 - V_{A_1} = \frac{2\left(F - C_1 + C_2\right) - (K_1 + S_2)}{2(F - Fd)} \tag{4.8}$$

Proposition 1. *The probability that enterprises choose compliance disclosure vulnerability behavior is positively correlated with the government's punishment, the additional benefits and losses from non-compliance, while it is negatively correlated with the cost savings from non-compliance disclosure.*

The proof is presented in the Appendix.

Proposition 1 suggests that enterprises' vulnerability disclosure behavior is influenced by their losses due to non-compliance. The government can reduce the frequency of enterprises' non-compliance disclosure behavior by increasing the degree of punishment. In addition, increasing enterprises' additional benefits and reducing losses can also encourage their positive behavior by establishing a collaborative vulnerability prevention and control mechanism, expanding the degree of vulnerability information sharing.

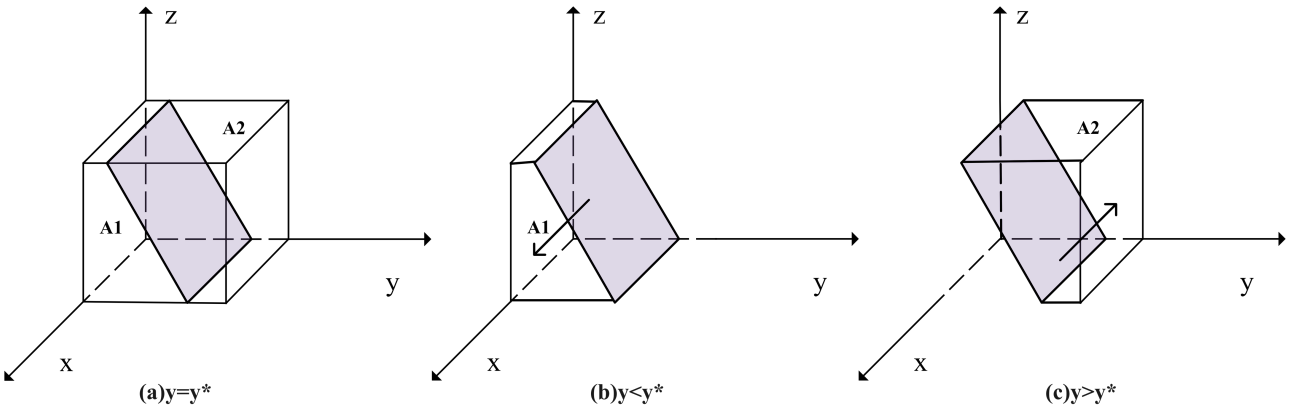


Figure 3. Phase diagram of strategy evolution for enterprises.

4.2. Stability analysis of TPCCTPs

According to Table 2, the expected income E_{21} or E_{22} of TPCCTPs when they choose the "active operation" or "negative operation" strategy are, respectively,

$$\begin{aligned} E_{21} = {} & xz\,(P_1 + P_2 - C_3 - C_4) + x(1-z)\,(P_1 - C_3 - C_4) + (1-x)z\,(P_1 + P_2 - C_3) \\ & + (1-x)(1-z)\,(P_1 - C_3) \end{aligned} \tag{4.9}$$

$$\begin{aligned} E_{22} = {} & xz\,(P_1 - C_3 - K_2 - F) + x(1-z)\,(P_1 - C_3 - F) + (1-x)z\,[P_1 - C_3 - K_2 - (1-d)F] \\ & + (1-x)(1-z)\,[P_1 - C_3 - (1-d)F] \end{aligned} \tag{4.10}$$

The average expected income $\overline{E_2}$ of TPCCTPs is

$$\overline{E_2} = yE_{21} + (1-y)E_{22} \tag{4.11}$$

According to Formulas (4.9)–(4.11), we can further obtain the replicator dynamics equation of the behavior strategy selection for TPCCTPs as follows:

$$F(y) = dy/dt = y\left(E_{21} - \overline{E_2}\right) = y(y-1)\,[Fd - F + (C_4 - Fd)\,x - (K_2 + P_2)\,z] \tag{4.12}$$

The first-order derivative of y is as follows:

$$\frac{d(F(y))}{dy} = (2y-1)\left[Fd - F + (C_4 - Fd)\,x - (K_2 + P_2)\,z\right] \tag{4.13}$$

Let $J(z) = (C_4 - Fd)\,x - (K_2 + S_2)\,z + Fd - F$. In order to find the probability of TPCCTPs choosing active operation behavior in the steady state, it must be satisfied that $F(y) = 0$ and $d(F(y))/dy < 0$, which results in $J(z)$ being a decreasing function.

When $z = Fd - F + (C_4 - Fd)\,x/(K_2 + S_2) = z^*$, $F(y) = 0$ and $d(F(y))/dy = 0$, all values of y are in the evolutionary steady state at this time. When $z < z^*$, $G(z) > 0$ and $d(F(y))/dy|_{y=0} < 0$, $y = 0$ is the evolutionary stabilization strategy for TPCCTPs. Otherwise, $y = 1$ is the evolutionary stabilization strategy. The evolutionary trend of strategy selection for TPCCTPs is shown in Figure 4.

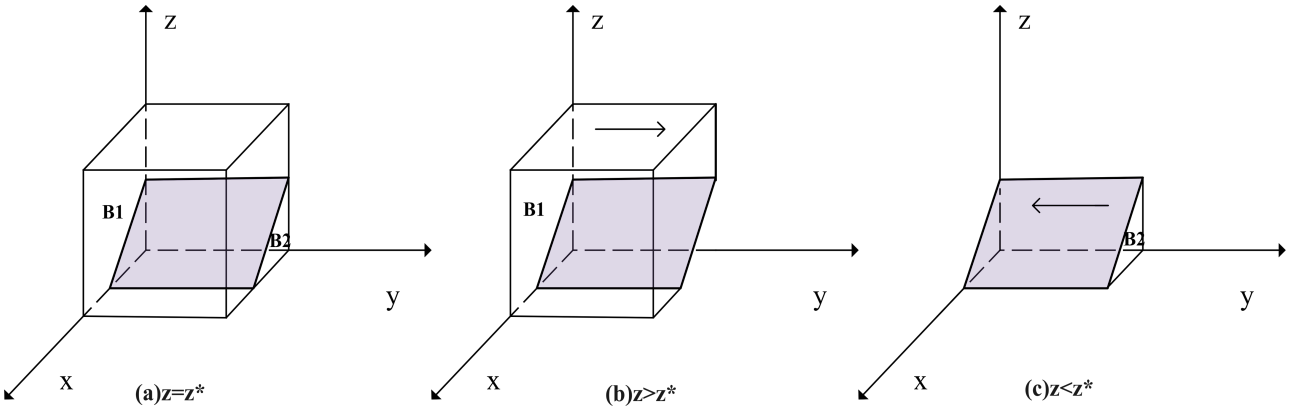


Figure 4. Phase diagram of strategy evolution for TPCCTPs.

From Figure 4, the tangent crosses the point $\left(\frac{F-Fd}{C_4-Fd}, 0, 0\right)$. The probability that TPCCTPs choose active operation behavior is V_{B_1} of B_1, and the probability that TPCCTPs choose negative operation behavior is V_{B_2} of B_2:

$$V_{B_2} = \int_0^0 \int_0^{\frac{F-Fd}{C_4-Fd}} \frac{Fd - F + (C_4 - Fd)\,x}{K_2 + S_2} dxdy = -\frac{(F-Fd)^2}{2\,(C_4 - Fd)\,(K_2 + S_2)} \tag{4.14}$$

$$V_{B_1} = 1 + \frac{(F-Fd)^2}{2\,(C_4 - Fd)\,(K_2 + S_2)} \tag{4.15}$$

Proposition 2. *The probability that TPCCTPs choose active operation behavior is positively correlated with the degree of the government punishment and the additional benefits of active operation, while it is negatively correlated with the collaborative costs and the losses of negative operation.*

The proof is presented in the Appendix.

Proposition 2 shows that if the government takes measures such as increasing policy support, cultivating talents and strengthening cybersecurity construction before TPCCTPs participate in

spontaneous collaborative disclosure, it will reduce TPCCTPs' collaborative costs and risks, which can increase their benefits. At this time, TPCCTPs are inclined to adopt active operation behavior for their own development.

4.3. Stability analysis of the government

Similarly, the expected income E_{31} or E_{32} of the government when they choose the "strict regulation" or "lax regulation" strategy are, respectively,

$$\begin{aligned} E_{31} = {} & xy\,(R + M - C_5) + x(1-y)\,(R + K_2 - C_5 - W) + (1-x)y\,(R + K_1 - C_5 - W) \\ & + (1-x)(1-y)\,(R + K_1 + K_2 - C_5 - W) \end{aligned} \tag{4.16}$$

$$E_{32} = xyM + x(1-y)(-W) + (1-x)y(-W) + (1-x)(1-y)(-W) \tag{4.17}$$

The average expected income $\overline{E_3}$ of the government is

$$\overline{E_3} = zE_{31} + (1-z)E_{32} \tag{4.18}$$

According to Formulas (4.16)–(4.18), we can further obtain the replicator dynamics equation for the behavior strategy selection of the government as follows:

$$F(z) = dz/dt = z\left(E_{31} - \overline{E_3}\right) = z(z-1)\,(C_5 - K_1 - K_2 - R + K_1 x + K_2 y) \tag{4.19}$$

The first-order derivatives of z and the set $H(y)$ are respectively given as follows:

$$\frac{d(F(z))}{dz} = (2z-1)\,(C_5 - K_1 - K_2 - R + K_1 x + K_2 y) \tag{4.20}$$

$$H(y) = C_5 - K_1 - K_2 - R + K_1 x + K_2 y \tag{4.21}$$

The condition that the government chooses strict regulation in a steady state must satisfy that $F(z) = 0$ and $d(F(z))/dz < 0$. Because $\partial H(y)/\partial y > 0$, $H(y)$ is an increasing function with respect to y.

When $y = C_5 - K_1 - K_2 - R + K_1 x/K_2 = y^{**}$, $H(y) = 0$ and $d(F(z))/dz = 0$, all values of z are in the evolutionary steady state at this time. When $y < y^{**}$, $H(y) < 0$ and $d(F(z))/\,dz|_{z=1} > 0$, $z = 1$ is the evolutionary stabilization strategy for the government. Otherwise, $z = 0$ is the evolutionary stabilization strategy. The evolutionary trend of strategy selection for the government is shown in Figure 5.

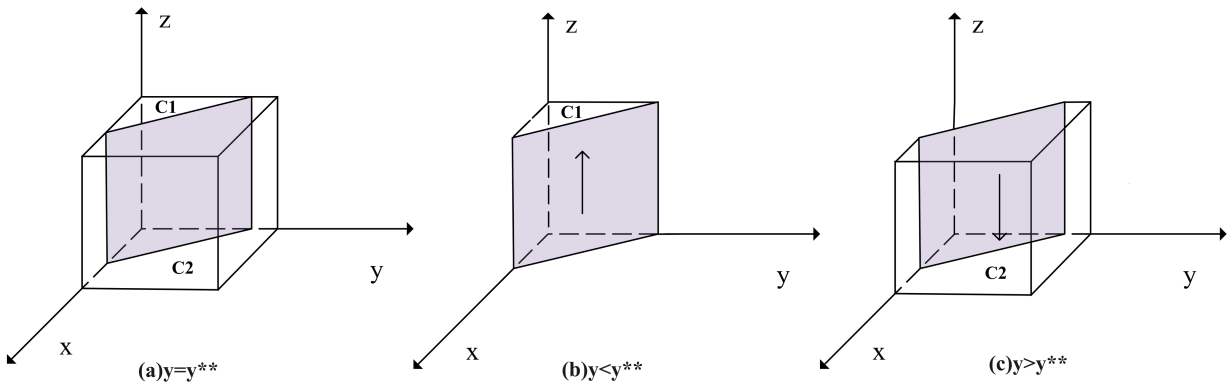


Figure 5. Phase diagram of strategy evolution for the government.

From Figure 5, the probability that the government imposes strict regulations is V_{C_1} of C_1:

$$V_{C_1} = \int_0^1 \int_0^1 \frac{C_5 - K_1 - K_2 - R + K_1 x}{K_2} dxdz = \frac{K_1 x - R - K_1 - K_2 + C_5}{K_2} \tag{4.22}$$

Proposition 3. *The probability that the government chooses strict regulation behavior is positively correlated with the government's punishment for enterprises and platforms, the regulatory benefits and social losses, while it is negatively correlated with the costs of strict regulation.*

The proof is presented in the Appendix.

Proposition 3 suggests that when enterprises engage in non-compliant disclosure behavior and TPCCTPs adopt negative operation behavior, it will result in significant social losses. In order to avoid such losses, the government always implements strict regulatory measures. However, if the regulatory costs are excessively high, it may reduce the likelihood that the government will adopt strict regulatory behavior, causing regulatory shortcomings.

4.4. Systematic equilibrium point analysis of the tripartite evolutionary game

The above equilibrium point does not comprehensively represent the evolutionary stability strategy for replicating a dynamic system. It is necessary to further discuss the stability of the system's equilibrium point by using the Jacobian matrix local stability analysis method. The Jacobian matrix of the tripartite evolutionary game system is as follows:

$$J = \begin{bmatrix} J_1 & J_2 & J_3 \\ J_4 & J_5 & J_6 \\ J_7 & J_8 & J_9 \end{bmatrix} = \begin{bmatrix} \partial F(x)/\partial x & \partial F(x)/\partial y & \partial F(x)/\partial z \\ \partial F(y)/\partial x & \partial F(y)/\partial y & \partial F(y)/\partial z \\ \partial F(z)/\partial x & \partial F(z)/\partial y & \partial F(z)/\partial z \end{bmatrix} \tag{4.23}$$

where

$$\begin{cases} J_1 = (2x-1)\left[C_1 - C_2 - Fd + (Fd - F)y - (K_1 + S_2)z\right] \\ J_2 = x(x-1)(Fd - F) \\ J_3 = x(x-1)(-K_1 - S_2) \\ J_4 = y(y-1)(C_4 - Fd) \\ J_5 = (2y-1)\left[Fd - F + (C_4 - Fd)x - (K_2 + S_2)z\right] \\ J_6 = y(y-1)(-K_2 - S_2) \\ J_7 = z(z-1)K_1 \\ J_8 = z(z-1)K_2 \\ J_9 = (2z-1)\left[C_5 - K_1 - K_2 - R + K_1 x + K_2 y\right] \end{cases} \tag{4.24}$$

The eigenvalues of the Jacobian matrix corresponding to the eight equilibrium points and the system stability are shown in Table 3.

Table 3. Each equilibrium point corresponds to the eigenvalue of the Jacobian matrix.

Equilibrium point	**Eigenvalue**			**Stability**
	λ_1	λ_2	λ_3	
$E_1(0,0,0)$	$C_2 - C_1 + Fd$	$F - Fd$	$K_1 - C_5 + K_2 + R$	Unstable point
$E_2(0,1,0)$	$C_2 - C_1 + F$	$Fd - F$	$K_1 - C_5 + R$	Unstable point
$E_3(0,0,1)$	$C_2 - C_1 + K_1 + S_2 + Fd$	$F + K_2 + P_2 - Fd$	$C_5 - K_1 - K_2 - R$	Unstable point
$E_4(0,1,1)$	$C_2 - C_1 + F + K_1 + S_2$	$Fd - K_2 - P_2 - F$	$C_5 - K_1 - R$	Stable point
$E_5(1,0,0)$	$C_1 - C_2 - Fd$	$F - C_4$	$K_2 - C_5 + R$	Stable point
$E_6(1,1,0)$	$C_1 - C_2 - F$	$C_4 - F$	$R - C_5$	Stable point
$E_7(1,0,1)$	$C_1 - C_2 - K_1 - S_2 - Fd$	$F - C_4 + K_2 + P_2$	$C_5 - K_2 + R$	Stable point
$E_8(1,1,1)$	$C_1 - C_2 - K_1 - S_2 - F$	$C_4 - F - K_2 - P_2$	$C_5 - R$	Stable point

It can be seen that the two equilibrium points $E_1(0,0,0)$ and $E_3(0,0,1)$ are never evolutionarily stable strategies under any conditions. On the one hand, this demonstrates that the cases in which enterprises, TPCCTPs and governments all adopt negative behaviors are relatively rare. On the other hand, it confirms that relying solely on strict governmental regulation does not result in the ideal state of the system. As for $E_2(0,1,0)$, due to TPCCTPs being profit-driven, when enterprises engage in non-compliance disclosure behaviors and the government adopts lax regulation behavior, TPCCTPs' external motivation for proactive disclosure is insufficient, making it almost impossible to choose active operation.

Furthermore, it is calculated that $E_8(1, 1, 1)$ is in a stable state. In this case, the government's regulatory policies and systems are relatively well-developed, with reduced regulatory costs and improved regulatory efficiency. For enterprises, under the continued drive of government regulation, the additional benefits of vulnerability disclosure provided by the government are relatively high. At this point, the cost gap between enterprises that adopt compliant disclosure behavior and non-compliant disclosure behavior is much smaller than the sum of the government punishments and the losses borne by the enterprise, i.e., $C_1 - C_2 < K_1 + S_2 + Fd$, so they choose compliance disclosure behavior. For TPCCTPs, their collaborative costs equate to less than the sum of government punishments, additional benefits and the losses borne by themselves, i.e., $C_4 < F + K_2 + P_2$, so TPCCTPs choose active operation behavior. This scenario can promote the healthy development of the crowdsourcing cybersecurity testing industry, where enterprises and TPCCTPs take positive vulnerability disclosure behaviors under the action of government regulation.

5. Simulation analysis

To verify the validity of evolutionary stability analysis and more intuitively describe the dynamic evolutionary process of enterprises, TPCCTPs and the government as they implement positive behaviors during crowdsourcing cybersecurity testing, we conducted numerical simulations by using MATLAB. Based on official data from HackerOne and Bugcrowd, the conditions that need to be satisfied are as follows: $C_1 - C_2 < K_1 + S_2 + F$, $C_4 < F + K_2 + P_2$, $C_5 < R$; the setting of each parameter value is as follows: $C_1 = 40$, $C_2 = 10$, $C_4 = 40$, $C_5 = 40$, $C_6 = 50$, $F = 20$, $d = 0.6$, $K_1 = 5$, $K_2 = 15$, $P_2 = 20$, $S_2 = 15$, $R = 60$, $W = 70$.

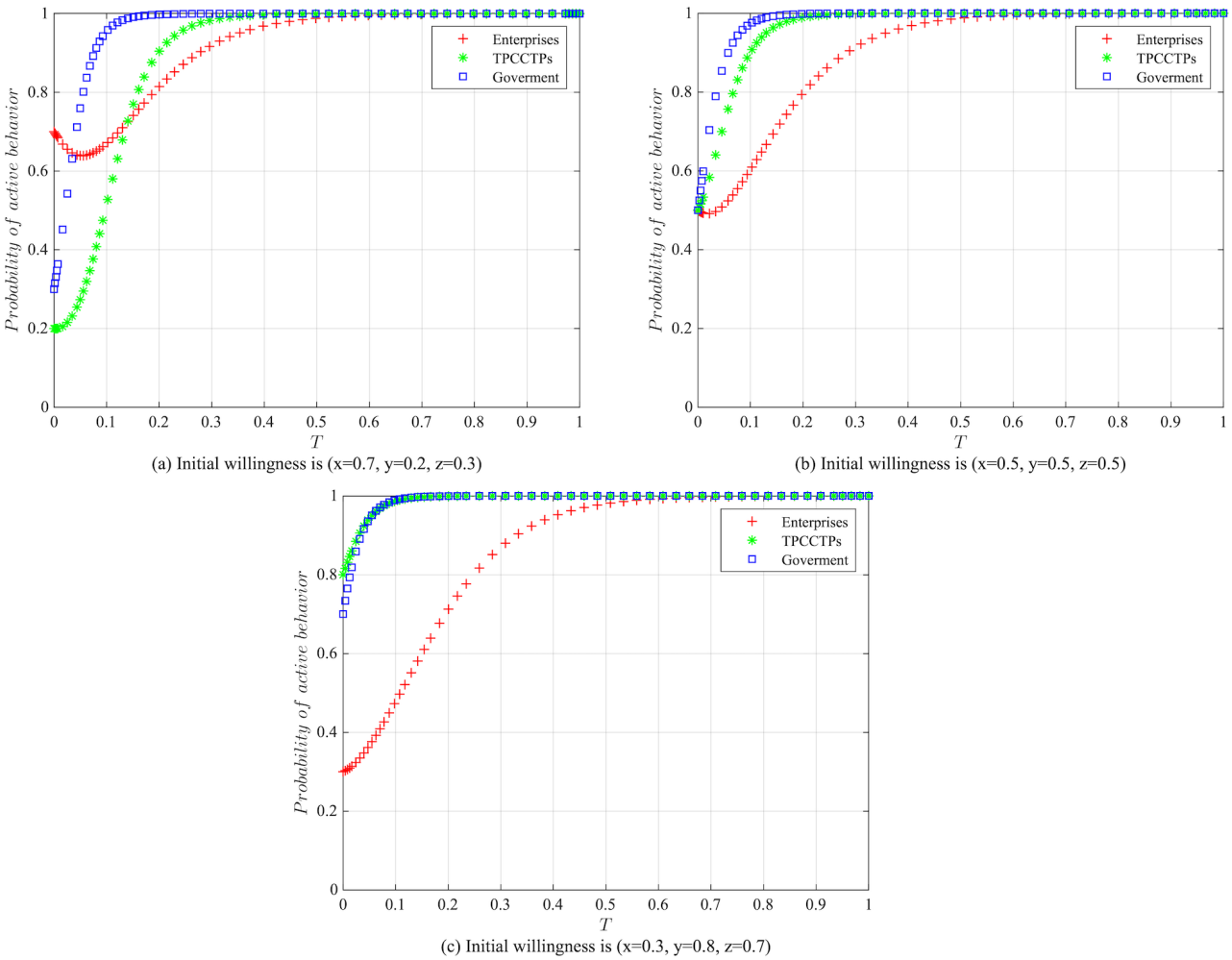
5.1. The impact of initial willingness on the system

Assuming that other parameters remain unchanged, we set the initial willingness of the three players to engage in positive behaviors as $(x = 0.7, y = 0.2, z = 0.3)$, $(x = 0.5, y = 0.5, z = 0.5)$, $(x = 0.3, y = 0.8, z = 0.7)$. The impact of the initial willingness of game players on the evolution of the system is shown in Figure 6. It can be seen from the figure that the initial willingness of the enterprises, TPCCTPs and government has no impact on the system's evolution strategy. The system consistently stabilizes with the positive behavior combination of {compliance disclosure, active operation, strict regulation}. However, the higher the initial willingness of the three players to choose positive behaviors, the faster the system reaches the positive behavior strategy combination. Therefore, it is evident that TPCCTPs should actively adhere to relevant regulations and rules in the early stages of platform establishment. The government should strengthen regulatory education for platforms and enterprises, guiding and standardizing their behaviors, which will encourage them to choose positive vulnerability disclosure behaviors.

5.2. The impact of the governmental regulation benefits on the system

Based on the initial willingness of $(x = 0.7, y = 0.2, z = 0.3)$, we set R to be 30 or 90. The impact of the governmental regulation benefits on the evolution of the system is shown in Figure 7. It can be observed that the governmental regulation benefits directly impact the evolutionary stability of the system. With the increase in governmental regulation benefits, the probability that the players will choose positive behaviors at the same time increases, and the time for the system to reach a

stable state is shortened. When governmental regulation benefits are low, the government may initially choose strict regulation to guide the vulnerability disclosure behavior of enterprises and TPCCTPs. However, as time progresses and regulatory benefits become insufficient to cover regulatory costs, the government may gradually ease its regulatory efforts, which could lead to enterprises and TPCCTPs gradually adopting negative behavior, hindering the system from reaching stability. Therefore, the government should implement various mechanisms to efficiently regulate vulnerability disclosure to reduce regulatory costs and enhance regulatory effectiveness. Additionally, the government should actively establish a positive regulatory image and improve its reputation to enhance the willingness of enterprises and TPCCTPs to cooperate with regulation, thereby increasing regulatory benefits.



(a) Initial willingness is (x=0.7, y=0.2, z=0.3)

(b) Initial willingness is (x=0.5, y=0.5, z=0.5)

(c) Initial willingness is (x=0.3, y=0.8, z=0.7)

Figure 6. The impact of initial willingness on evolutionary results.

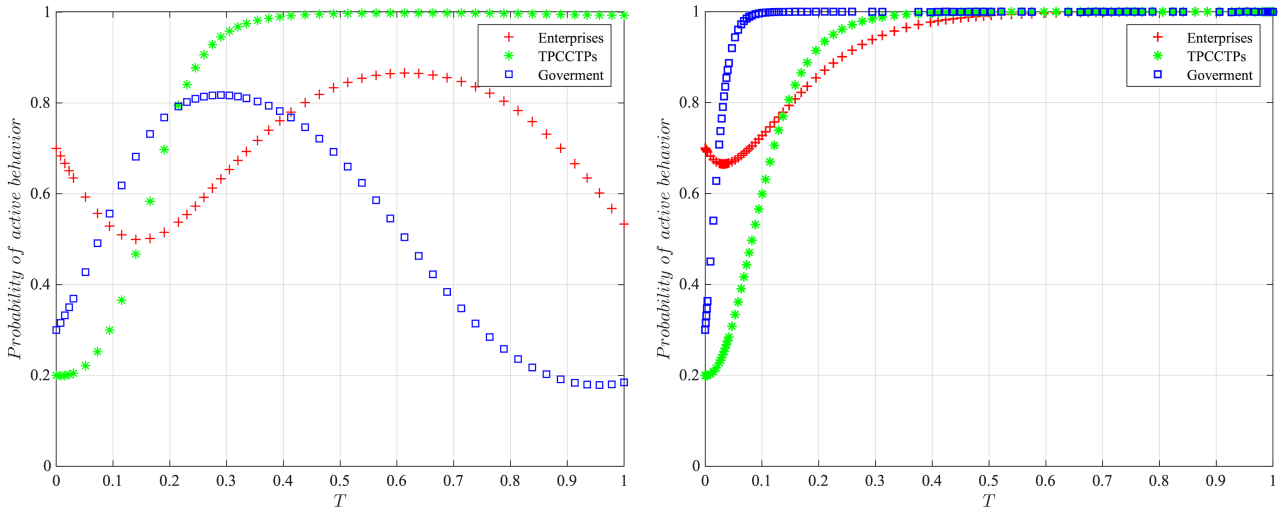
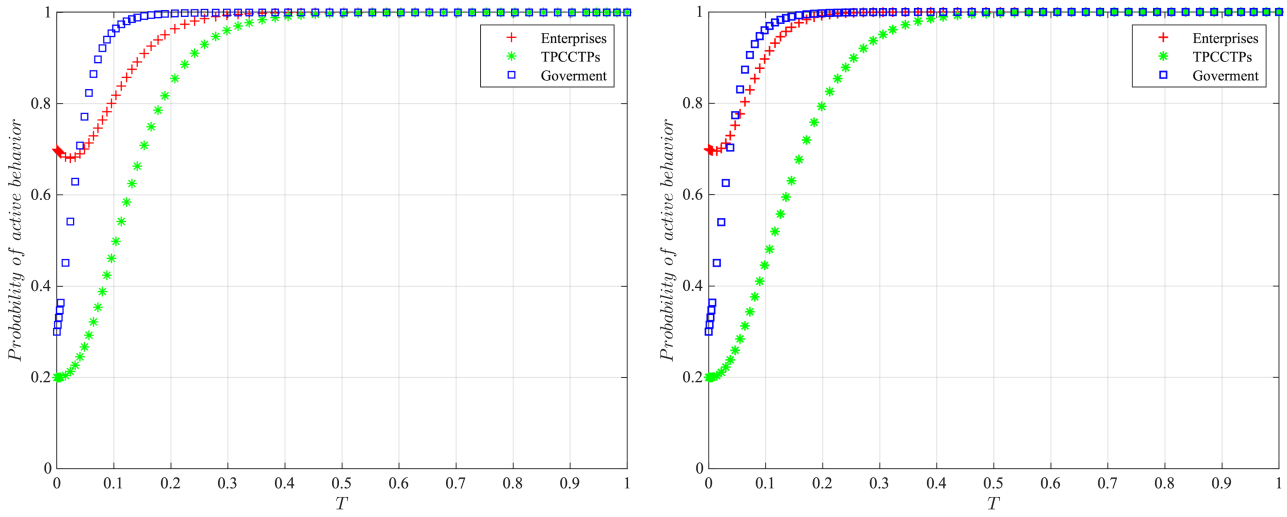


Figure 7. The impact of the governmental regulation benefits on evolutionary results.

5.3. The impact of the punishment mechanism on the system

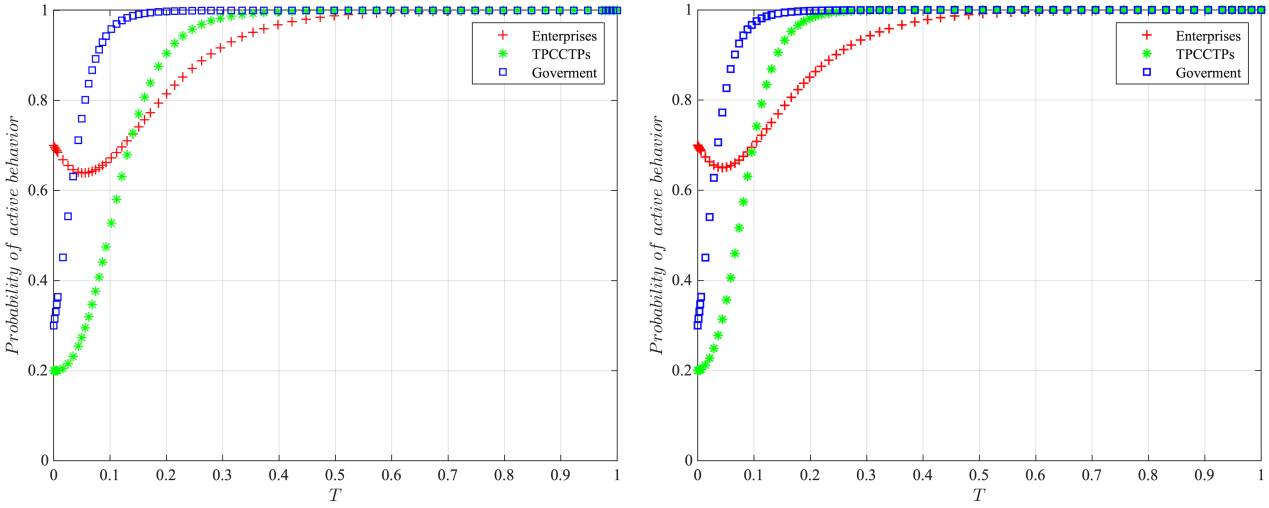
Based on the above analysis, we investigated the impact of the punishment mechanism on the stability of system evolution from two aspects, i.e., the government's punishments for enterprises and the government's punishments for TPCCTPs. First, assuming other variables remain unchanged, we set the government's punishments for enterprises K_1 to 15 or 25, and the impact on the evolution of the system is shown in Figure 8. It is evident that although the government punishments for enterprises have no impact on the system's stable state, which consistently stabilizes at the point of $(1, 1, 1)$, it impacts the speed of evolution of vulnerability disclosure behaviors of enterprises and TPCCTPs from the initial state to the stable state. Specifically, when the government dramatically increases punishments for enterprises, enterprises accelerate their compliant disclosure behavior, while TPCCTPs retard their active operation behavior. This indicates that punishments for enterprises are essential for promoting enterprises' positive behavior, but they have a restraining effect on TPCCTPs' behavior. Therefore, from an overall perspective, increasing punishments for enterprises is beneficial only when the impact of the vulnerability disclosure behavior of enterprises significantly outweighs that of TPCCTPs.

To further investigate the impact of the government's punishment for TPCCTPs on system evolution, we set K_2 to 15 or 25, and the results are shown in Figure 9. Similarly, an increase in government punishments for platforms has no impact on the system's stable state, and it influences the speed of evolution of vulnerability disclosure behaviors of enterprises and TPCCTPs. When the government increases penalties for enterprises, enterprises and TPCCTPs adopt positive behavior more rapidly. Compared to government punishments for enterprises, although increasing punishments for platforms can incentivize both players, the extent of this response is relatively lesser. Therefore, when the government tends to promote positive behavior in enterprises and TPCCTPs in a non-urgent manner, increasing punishments for platforms becomes more effective from a long-term perspective.



(a) K1=15 (b) K1=25

Figure 8. The impact of the government's punishments in terms of the enterprises on evolutionary results.



(a) K2=15 (b) K2=25

Figure 9. The impact of the government's punishments in terms of the TPCCTPs on evolutionary results.

5.4. The impact of the subsidy mechanism on the system

Based on the above analysis, we investigated the impact of the subsidy mechanism on the stability of system evolution from two aspects, i.e., enterprises' additional benefits and TPCCTPs' additional benefits. First, assuming other variables remain unchanged, we set the enterprises' additional benefits S_2 to 5 or 25, and its impact on the evolution of the system is shown in Figure 10. It can be observed that enterprises' additional benefits directly impact the evolutionarily stable strategy of enterprises. When enterprises' additional benefits are relatively low, the driving force for enterprises to adopt positive behavior is insufficient, and the system cannot reach a stable state. When the additional

benefits are sufficiently high, enterprises are highly motivated to engage in compliant disclosure behavior. Meanwhile, this leads to the system ultimately reaching a stable state wherein all players engage in positive behavior. However, TPCCTPs' response to increased additional benefits for enterprises is minimal, as it consistently reaches its stable state at a certain rate. This indicates that enterprises' additional benefits primarily impact their own behavioral strategies, allowing the system to evolve rapidly, with little effect on TPCCTPs' behavior. Therefore, the government can enhance subsidy mechanisms for enterprises to incentivize their behavior, including measures such as establishing a vulnerability coordination response process, promoting vulnerability sharing platforms and increasing subsidies for compliant enterprises.

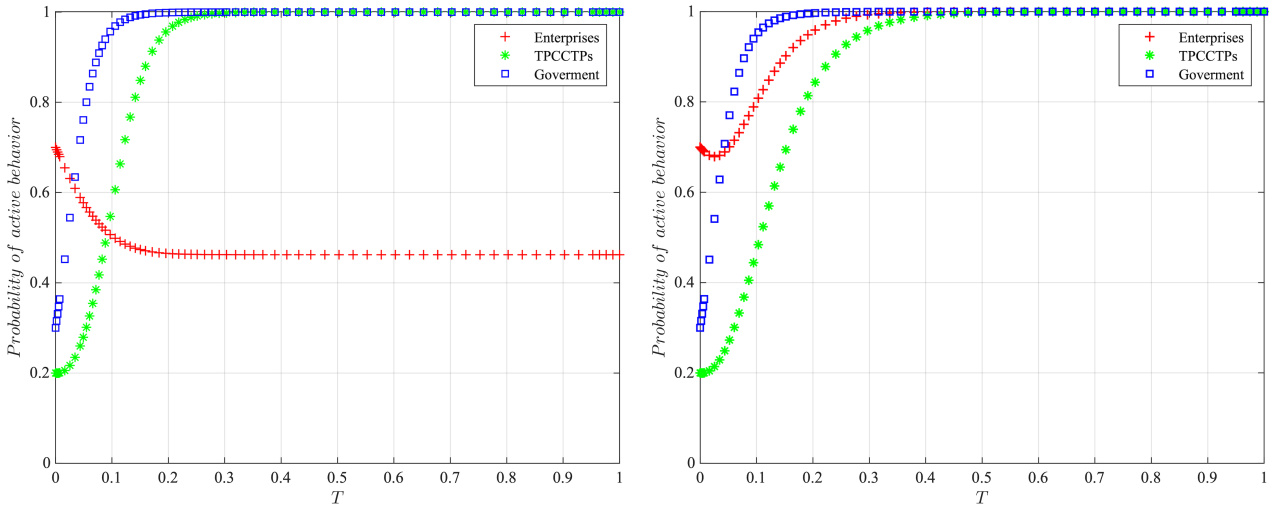
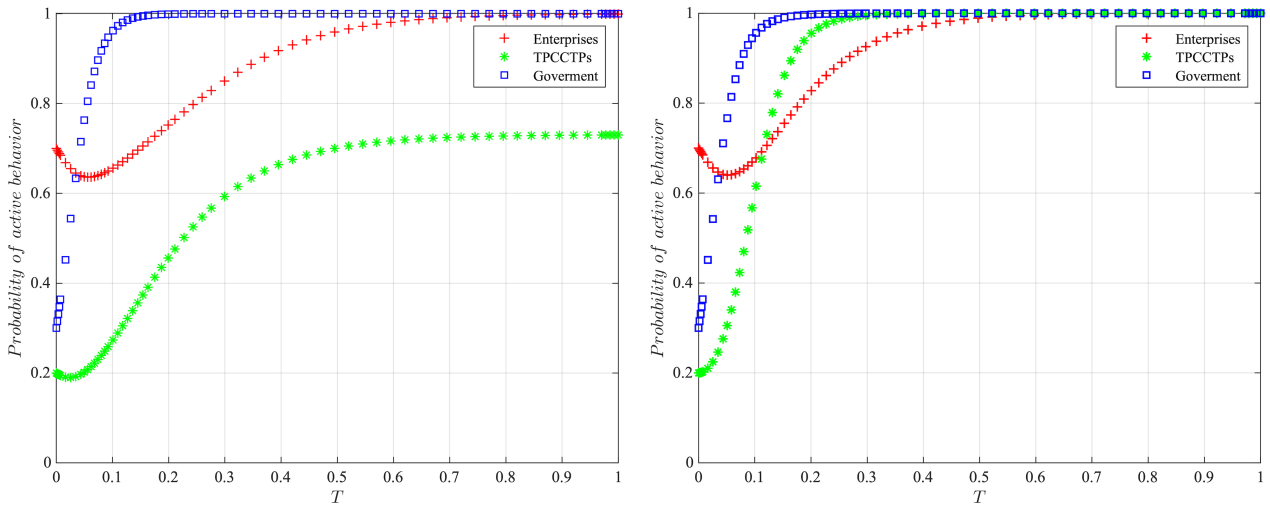


Figure 10. The impact of enterprises' additional benefits on evolutionary results.

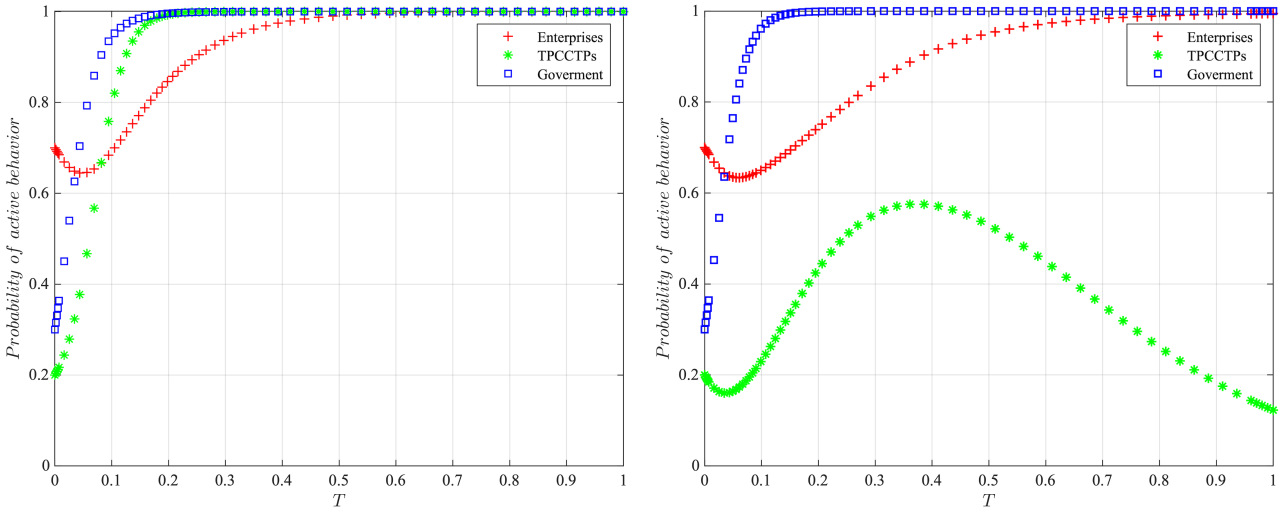
Additionally, we set P_2 to 5 or 25 and investigated the impact of TPCCTPs' additional benefits on system evolution as shown in Figure 11. We have found that TPCCTPs' additional benefits not only impact its own evolutionarily stable strategy, but they also affect the speed of evolution of enterprises' behavior. When TPCCTPs' additional benefits are relatively low, their testing costs are much higher than the benefits of active operation and the risks of negative operation. In this case, the probability of the platform adopting positive behavior inevitably decreases, causing the system to evolve into an ineffective state of {compliance disclosure, negative operation, strict regulation}. Meanwhile, due to the TPCCTPs' lack of cooperation, the speed of enterprises' compliance disclosure behavior decreases. When TPCCTPs' additional benefits are sufficiently high, they are motivated to engage in active operation and the system evolves to a stable state wherein all players engage in positive behavior. At the same time, the evolutionary stability time for enterprises is shortened, allowing the system to reach a stable state faster than the baseline model. Compared to providing subsidies for enterprises, improving TPCCTPs' subsidies is more effective and can incentivize both players to engage in positive behaviors. Therefore, the government should pay more attention to TPCCTPs' subsidy mechanism and implement measures such as enhancing vulnerability disclosure regulations, optimizing the vulnerability disclosure process and increasing platform vulnerability testing subsidies to incentivize TPCCTPs' vulnerability disclosure behavior to stimulate their crucial role in the

development of crowdsourcing cybersecurity testing.



(a) P2=5 (b) P2=25

Figure 11. The impact of enterprises' additional benefits on evolutionary results.



(a) C4=20 (b) C4=60

Figure 12. The impact of enterprises' additional benefits on evolutionary results.

5.5. The impact of the collaborative disclosure mechanism on the system

Furthermore, we investigated the impact of the collaborative disclosure mechanism on the stability of system evolution from the perspective of TPCCTPs' collaborative costs. Assuming other variables remain unchanged, we set C_4 to 20 or 60; the impact of collaborative costs on the evolution of the system is shown in Figure 12. When TPCCTPs' collaborative costs are relatively low, they do not need to cover excessive costs to collaborate in the area of vulnerability disclosure; also, the system can reach a stable state faster than the baseline model. Meanwhile, the time for enterprises to evolve into a stable state of compliance disclosure behavior is shortened. When TPCCTPs' collaborative

costs are excessive, the additional benefits brought by collaborative vulnerability disclosure cannot offset the costs incurred, consequently diminishing the TPCCTPs' motivation for collaborative disclosure and significantly slowing down the speed of evolution of enterprise compliance disclosure behavior. In this case, the system evolves to an ineffective state. To avoid this, the government should establish a reasonable collaborative disclosure mechanism based on encouraging collaborative disclosure, simplify the vulnerability disclosure process to reduce collaborative costs and promote the development of collaborative vulnerability disclosure by increasing the TPCCTPs' willingness to participate.

6. Conclusions and future research

6.1. Conclusions

The emergence of crowdsourcing cybersecurity testing has reduced the obstacles to vulnerability disclosure, but it has also brought problems such as non-compliant vulnerability disclosure and conflicts of interests among the participants. It is indispensable to research the regulatory mechanisms of vulnerability disclosure behaviors in the setting of crowdsourcing cybersecurity testing. Therefore, based on game theory, this paper explores the evolutionary process of behavioral strategies for enterprises, TPCCTPs and the government. Subsequently, numerical simulations conducted by using MATLAB were presented to investigate the impact of various regulatory mechanisms on evolutionary stability.

We have discovered the following conclusions. First, the initial willingness of enterprises, TPCCTPs and governments has no influence on the system's stable state, which consistently evolves into a combination of positive behaviors, manifested in the form of {compliance disclosure, active operation, strict regulation}. The higher the initial willingness to adopt positive behaviors, the faster the system reaches the optimal combination of positive behaviors. However, when the governmental regulation benefit is low, the system cannot reach stability. Second, although increasing government punishments for enterprises and TPCCTPs does not affect the system's stability, it impacts the speed of evolution of behaviors for enterprises and TPCCTPs from the initial state to the stable state. Specifically, when punishments for enterprises are increased, enterprises significantly accelerate their adoption of positive behaviors, while TPCCTPs tend to reduce the speed of adopting positive behaviors. When punishments for TPCCTPs are increased, both players adopt positive behaviors more rapidly. Compared to increasing punishments for enterprises, enhancing punishments for TPCCTPs provides incentives to both players, with a relatively low response extent. Third, the additional benefits that enterprises and TPCCTPs receive from subsidy mechanisms impact the system's stable evolutionary strategy and the speed of evolution of their behaviors. The system can be driven to a steady state only if the additional benefits to the enterprise and TPCCTPs are sufficiently high; it will evolve into an ineffective state otherwise. Compared to enterprises' additional benefits, TPCCTPs' additional benefits can simultaneously incentivize both players to adopt positive behaviors. In other words, improving the subsidy mechanism for TPCCTPs is more effective in promoting the system's evolution. Fourth, when TPCCTPs incur excessive collaborative costs, the additional benefits derived from TPCCTPs' collaborative disclosure are insufficient to cover their costs, and the motivation to engage in collaborative vulnerability disclosure for them is lacking, which results in the system evolving into an ineffective state.

To regulate the vulnerability disclosure behaviors of all participants and achieve the goal of collaborative vulnerability disclosure, the government can implement the following measures. First of all, the government should enhance regulatory education for enterprises and TPCCTPs and actively implement various regulatory mechanisms to enhance the government's credibility. This will increase the willingness of enterprises and TPCCTPs to cooperate with regulation, which can reduce regulatory costs and increase regulatory benefits, resulting in efficient regulation. Next, the government should implement targeted punishment mechanisms based on the characteristics of different stages of vulnerability disclosure. In the early stages of regulation, when enterprises have serious vulnerability disclosure issues, the government should primarily increase punishments for enterprises to swiftly address the problem. As vulnerability disclosure behavior gradually becomes more standardized, the government should reduce punishments for enterprises and slightly increase the regulation of TPCCTPs. This approach aims to promote positive vulnerability disclosure behaviors from both participants by enhancing the process of crowdsourcing cybersecurity testing services. When vulnerability disclosure behavior becomes positive and stable, the government can gradually reduce punishments and establish a good market environment for voluntary disclosure. Then, the government should implement a subsidy mechanism of TPCCTPs as primary and enterprises as secondary. Measures such as improving vulnerability disclosure regulations, optimizing the vulnerability disclosure process and increasing subsidies for TPCCTPs' vulnerability testing should be implemented to reduce the vulnerability disclosure risks faced by TPCCTPs' hackers, which will help to create a favorable atmosphere of hackers actively engaging and platforms actively operating for crowdsourcing cybersecurity testing services. Finally, the government should encourage enterprises, white-hat hackers, TPCCTPs and other stakeholders to collaborate in the area of disclosing vulnerabilities and improve the collaborative disclosure mechanisms. To reduce TPCCTPs' cost of collaborative disclosure, various measures should be implemented, including establishing a vulnerability information sharing system, enhancing a multi-party emergency response system and improving the social credit system. This will ensure the TPCCTPs' stable development, which promotes the continuous improvement of crowdsourcing cybersecurity testing.

6.2. Future research

This paper provides a theoretical foundation and practical recommendations for the governmental regulation of participants' vulnerability disclosure behaviors in the setting of crowdsourcing cybersecurity testing. However, it is worth further study. On one hand, vulnerability disclosure in the setting of crowdsourcing cybersecurity testing is a complex process involving multiple stakeholders, while we only focused on the core participants involved in vulnerability disclosure and did not consider various types and characteristics of participants in the market. Future research should explore a broader range of participants, taking the public and the media into account, or considering the homogeneity or heterogeneity of enterprises or TPCCTPs. On the other hand, this paper's depiction of the crowdsourcing cybersecurity testing environment is not sufficiently detailed, as it simplifies the research problem by assuming cooperation between enterprises and TPCCTPs, as well as between TPCCTPs and white-hat hackers. In fact, there is intense competition among enterprises, TPCCTPs and white-hat hackers. In future research, it may be worthwhile to analyze vulnerability disclosure issues in the setting of crowdsourcing cybersecurity testing from a competitive perspective, considering the preferences and attributes of different participants.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This research was supported by the Humanities and Social Science Foundation of the Ministry of Education of China (Grant No. 22YJC630214) and the National Natural Science Foundation of China (Grant No. 71801125).

Conflict of interest

The authors declare that there is no conflict of interest.

References

1. Y. S. Pil, *The Way Forward for Security Vulnerability Disclosure Policy: Comparative Analysis of US, EU, and Netherlands*, (2013), 119–131, https://doi.org/10.1007/978-3-031-19608-9_10
2. M. Zhao, A. Laszka, T. Maillart, J. Grossklags, Crowdsourced security vulnerability discovery: Modeling and organizing bug-bounty programs, in *The HCOMP Workshop on Mathematical Foundations of Human Computation, Austin, TX, USA*, 2016.
3. T. Maillart, M. Zhao, J. Grossklags, J. Chuang, Given enough eyeballs, all bugs are shallow? revisiting eric raymond with bug bounty programs, *J. Cybersecur.*, **3** (2017), 81–90. https://doi.org/10.1093/cybsec/tyx008
4. X. Liu, Y. Zhang, H. Zhang, X. Cheng, The practice, achievements, and enlightenment of bug bounty programs of the U.S. department of defense, *Natl. Defense Technol.*, **40** (2019).
5. M. Zhao, A. Laszka and J. Grossklags, Devising effective policies for bug-bounty platforms and security vulnerability discovery, *J. Inf. Policy*, **7** (2017), 372–418. http://doi.org/10.5325/jinfopoli.7.2017.0372
6. U. Ķinis, From responsible disclosure policy (rdp) towards state regulated responsible vulnerability disclosure procedure (hereinafter–rvdp): The latvian approach, *Comput. Law Secur. Rev.*, **34** (2018), 508–522. https://doi.org/10.1016/j.clsr.2017.11.003
7. A. Arora, R. Telang, H. Xu, Optimal policy for software vulnerability disclosure, *Manage. Sci.*, **54** (2008), 642–656. https://doi.org/10.1287/mnsc.1070.0771
8. A. M. Algarni, Y. K. Malaiya, Software vulnerability markets: Discoverers and buyers, *Int. J. Comput. Inf. Eng.*, **8** (2014), 480–490. https://doi.org/10.5281/zenodo.1091516
9. A. Arora, R. Krishnan, R. Telang, Y. Yang, An empirical analysis of software vendors' patch release behavior: impact of vulnerability disclosure, *Inf. Syst. Res.*, **21** (2010), 115–132. https://doi.org/10.1287/isre.1080.0226
10. J. Ruohonen, L. Allodi, A bug bounty perspective on the disclosure of web vulnerabilities, preprint, arXiv:1805.09850.

11. M. Al-Banna, B. Benatallah, D. Schlagwein, E. Bertino, M. C. Barukh, Friendly hackers to the rescue: How organizations perceive crowdsourced vulnerability discovery, in *PACIS*, (2018), 230. https://doi.org/https://aisel.aisnet.org/pacis2018
12. A. M. Jo, Hackers' self-selection in crowdsourced bug bounty programs, *Rev. Econ. Ind.*, **172** (2020), 83–132.
13. E. Rudenko, A. Gnatenko, A. Milich, K. Hedgecock, Z. M. Smith, Leveraging ethical hacking in russia: Exploring the design and potential of bug bounty programs, in *Stanford US-Russia Forum Journal*, **12** (2020).
14. A. Dingman, G. Russo, Risk-based vulnerability disclosure: Towards optimal policy, *SSRN*, **2015** (2015). https://doi.org/10.2139/ssrn.2601191
15. A. Arora, R. Krishnan, A. Nandkumar, R. Telang, Y. Yang, Impact of vulnerability disclosure and patch availability-an empirical analysis, in *Third Workshop on the Economics of Information Security*, **24** (2004), 1268–1287.
16. J. Radianti, Eliciting information on the vulnerability black market from interviews, in *2010 Fourth International Conference on Emerging Security Information, Systems and Technologies*, (2010), 154–159. https://doi.org/10.1109/SECURWARE.2010.33
17. A. Arora, R. Telang, Economics of software vulnerability disclosure, *IEEE Secur. Privacy*, **3** (2005), 20–25. https://doi.org/10.1109/MSP.2005.12
18. A. Ahmed, B. Lee, Organizational learning on bug bounty platforms, in *26th Americas Conference on Information Systems, AMCIS*, 2020.
19. H. Cavusoglu, H. Cavusoglu, J. Zhang, Security patch management: Share the burden or share the damage?, *Manage. Sci.*, **54** (2008), 657–670. https://doi.org/10.1287/mnsc.1070.0794
20. S. Parker, Z. Wu, P. D. Christofides, Cybersecurity in process control, operations, and supply chain, *Comput. Chem. Eng.*, **171** (2023), 108169. https://doi.org/10.1016/j.compchemeng.2023.108169 .
21. A. Arora, A. Nandkumar, R. Telang, Does information security attack frequency increase with vulnerability disclosure? An empirical analysis, *Inf. Syst. Front.*, **8** (2006), 350–362. https://doi.org/10.1007/s10796-006-9012-5
22. S. Ransbotham, S. Mitra, J. Ramsey, Are markets for vulnerabilities effective?, *MIS Q.*, **36** (2012), 43–64. https://doi.org/10.2307/41410405
23. E. Rescorla, Is finding security holes a good idea?, *IEEE Secur. Privacy*, **3** (2005), 14–19. https://doi.org/10.1109/MSP.2005.17
24. H. Cavusoglu, B. Mishra, S. Raghunathan, The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers, *Int. J. Electr. Commer.*, **9** (2004), 70–104. https://doi.org/10.1080/10864415.2004.11044320
25. R. Telang, S. Wattal, An empirical analysis of the impact of software vulnerability announcements on firm stock price, *IEEE Trans. Software Eng.*, **33** (2007), 544–557. https://doi.org/10.1109/TSE.2007.70712
26. S. Mitra, S. Ransbotham, Information disclosure and the diffusion of information security attacks, *Inf. Syst. Res.*, **26** (2015), 565–584. https://doi.org/10.1287/isre.2015.0587

27. R. Böhme, L. Eckey, T. Moore, N. Narula, T. Ruffing, A. Zohar, Responsible vulnerability disclosure in cryptocurrencies, *Commun. ACM*, **63** (2020), 62–71. https://doi.org/10.1145/3372115
28. S. P. Gayialis, E. P. Kechagias, G. A. Papadopoulos, E. Kanakis, A smart-contract enabled blockchain traceability system against wine supply chain counterfeiting, in *Advances in Production Management Systems. Smart Manufacturing and Logistics Systems: Turning Ideas into Action*, (2022), 477–484. https://doi.org/10.1007/978-3-031-16407-1_56
29. S. P. Gayialis, E. P. Kechagias, G. A. Papadopoulos, N. A. Panayiotou, A business process reference model for the development of a wine traceability system, *Sustainability*, **14** (2022), 11687. https://doi.org/10.3390/su141811687
30. E. P. Kechagias, S. P. Gayialis, G. A. Papadopoulos, G. Papoutsis, An ethereum-based distributed application for enhancing food supply chain traceability, *Foods*, **12** (2023), 1220. https://doi.org/10.3390/foods12061220
31. M. Mijwil, M. Aljanabi, ChatGPT, Towards artificial intelligence-based cybersecurity: The practices and chatgpt generated ways to combat cybercrime, *Iraqi J. Comput. Sci. Math.*, **4** (2023), 65–70. https://doi.org/10.52866/ijcsm.2023.01.01.0019
32. A. T. Chatfield, C. G. Reddick, Crowdsourced cybersecurity innovation: The case of the pentagon's vulnerability reward program, *Inf. Polity*, **23** (2018), 177–194. https://doi.org/https://doi.org/10.3233/IP-170058
33. K. Kannan, R. Telang, Market for software vulnerabilities? think again, *Manage. Sci.*, **51** (2005), 726–740. https://doi.org/10.1287/mnsc.1040.0357
34. C. Pascariu, Getting started with vulnerability disclosure and bug bounty programs, *Int. J. Inf. Secur. Cyber.*, **11** (2022), 25–30. https://www.ceeol.com/search/article-detail?id=1096780
35. M. Zhao, J. Grossklags, K. Chen, An exploratory study of white hat behaviors in a web vulnerability disclosure program, in *Proceedings of the 2014 ACM workshop on security information workers*, (2014), 51–58. https://doi.org/10.1145/2663887.2663906
36. T. L. Huber, T. A. Fischer, J. Dibbern, R. Hirschheim, A process model of complementarity and substitution of contractual and relational governance in is outsourcing, *J. Manage. Inf. Syst.*, **30** (2013), 81–114. https://doi.org/10.2753/MIS0742-1222300304
37. J. T. Lind, H. Mehlum, With or without u? the appropriate test for a u-shaped relationship*, *Oxford Bull. Econ. Stat.*, **72** (2010), 109–118. https://doi.org/10.1111/j.1468-0084.2009.00569.x
38. D. Luna, L. Allodi, M. Cremonini, Productivity and patterns of activity in bug bounty programs: Analysis of hackerone and google vulnerability research, in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, (2019), 1–10. https://doi.org/10.1145/3339252.3341495
39. M. Finifter, D. Akhawe, D. A. Wagner, An empirical study of vulnerability rewards programs, in *Proceedings of the 22nd USENIX Conference on Security*, (2013), 273–288.
40. J. Zhou, S. Wang, C. P. Bezemer, Y. Zou, A. E. Hassan, Studying the association between bountysource bounties and the issue-addressing likelihood of github issue reports, *IEEE Trans. Software Eng.*, **47** (2021), 2919–2933. http://doi.org/10.1109/TSE.2020.2974469

41. D. Votipka, R. Stevens, E. Redmiles, J. Hu, M. Mazurek, Hackers vs. testers: A comparison of software vulnerability discovery processes, in *2018 IEEE Symposium on Security and Privacy (SP)*, (2018), 374–391. http://doi.org/10.1109/SP.2018.00003

42. A. Ahmed, B. Lee, A. V. Deokar, The role of vulnerability disclosure on hacker participation in bug bounty programs, in *ICIS 2021 Proceedings*, (2021), 14.

43. Q. Xiong, Y. Zhu, Z. Zeng, X. Yang, Signal game analysis between software vendors and third-party platforms in collaborative disclosure of network security vulnerabilities, *Complexity*, **2023** (2023), 1027215. http://doi.org/10.1155/2023/1027215

44. L. Xu, Y. Li, Q. Yao, Information security investment and purchase decision for personalized products, *Managerial Decis. Econ.*, **43** (2022), 2619–2635. https://doi.org/10.1002/mde.3551

45. T. Walshe, A. Simpson, Coordinated vulnerability disclosure programme effectiveness: Issues and recommendations, *Comput. Secur.*, **123** (2022), 102936 https://doi.org/10.1016/j.cose.2022.102936

46. Q. Xiong, S. Lian, Z. Zeng, An empirical analysis of vulnerability information disclosure impact on patch r&d of software vendors, *J. Intell. Fuzzy Syst.*, **44** (2023), 839–853. https://doi.org/10.3233/JIFS-221316

47. S. Atefi, A. Sivagnanam, A. Ayman, J. Grossklags, A. Laszka, The benefits of vulnerability discovery and bug bounty programs: Case studies of chromium and firefox, in *Proceedings of the ACM Web Conference 2023*, (2023), 2209–2219. https://doi.org/10.1145/3543507.3583352

48. S. A. McCartney, *A Framework to Assess Bug-Bounty Platforms Based on Potential Attack Vectors*, PhD thesis, Montana State University-Bozeman, College of Engineering, 2022.

Appendix

Proof of Proposition 1. The probability that enterprises choose compliance disclosure vulnerability is V_{A_2}, while the first-order partial derivatives of each element are as follows: $\partial V_{A_2}/\partial F > 0$, $\partial V_{A_2}/\partial(K_1 + S_2) > 0$, $\partial V_{A_2}/\partial Fd > 0$, $\partial V_{A_2}/\partial(C_1 - C_2) > 0$. Thus, an increase in $(K_1 + S_2)$, F and Fd or a decrease in $(C_1 - C_2)$ can increase the probability of the compliance disclosure of enterprises. □

Proof of Proposition 2. Based on the expression for the probability V_{B_1} that TPCCTPs are active operations, the first-order partial derivatives of each element can be obtained: $\partial V_{B_1}/\partial(K_2 + S_2) > 0$, $\partial V_{B_1}/\partial F > 0$, $\partial V_{B_1}/\partial Fd > 0$, $\partial V_{B_1}/\partial C_4 > 0$. Thus, a decrease in Fd and C_4, and an increase in $(K_2 + S_2)$ and F, can both lead to an increase in the probability of active operation of TPCCTPs. □

Proof of Proposition 3. According to V_{C_1}, the first-order partial derivatives of each element can be obtained separately, as follows: $\partial V_{C_1}/\partial(K_1 + K_2) > 0$, $\partial V_{C_1}/\partial R > 0$, $\partial V_{C_1}/\partial W > 0$, $\partial V_{C_1}/\partial C_5 > 0$. Therefore, an increase in $(K_1 + K_2)$, R and W and a decrease in C_5 increases the probability of the government enacting strict regulations. □