E-Commerce Letters 电子商务评论, 2025, 14(5), 1742-1751
Published Online May 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.1451456

Hans汉斯

基于序贯博弈的第三方漏洞共享平台信息安全漏洞披露策略分析

宋倩文

江苏大学管理学院，江苏 镇江

收稿日期：2025年4月9日；录用日期：2025年4月23日；发布日期：2025年5月23日

摘　要

全球网络威胁日趋严峻，作为网络安全事件产生的根源之一，信息安全漏洞逐渐成为各国网络空间安全战略的重要内容，对信息安全漏洞的披露已是国家网络安全应急体系建设的重要内容之一。本文运用序贯博弈理论深入剖析信息安全漏洞披露中软件供应商、第三方漏洞共享平台、黑客及用户间的漏洞披露策略，揭示各方在不同情境下的最优策略，明晰信息不对称、成本收益等因素对决策的影响。研究发现，软件供应商在权衡成本与声誉损失后决策补丁披露；平台依据信息优势与收益决定漏洞公开；黑客基于入侵成功率和收益实施攻击；用户依据漏洞风险评估选择是否修复。本文为优化漏洞披露机制、提升信息安全管理水平提供理论支撑，对完善信息安全治理体系意义重大。

关键词

信息安全，序贯博弈理论，漏洞披露，信息不对称

Analysis of Information Security Vulnerabilities Disclosure Strategy for Third Party Vulnerability Sharing Platform Based on Sequential Game Theory

Qianwen Song

School of Management, Jiangsu University, Zhenjiang Jiangsu

Received: Apr. 9th, 2025; accepted: Apr. 23rd, 2025; published: May 23rd, 2025

Abstract

Global cyber threats are becoming increasingly severe, as one of the root causes of network security

文章引用: 宋倩文. 基于序贯博弈的第三方漏洞共享平台信息安全漏洞披露策略分析[J]. 电子商务评论, 2025, 14(5): 1742-1751. DOI: 10.12677/ecl.2025.1451456

incidents, information security vulnerabilities have gradually become an important part of Cyberspace Security Strategies in various countries. Disclosing information security vulnerabilities has become an important part of national network security emergency system construction. This paper uses sequential game theory to analyze the vulnerability disclosure strategies among software vendors, third-party vulnerability sharing platforms, hackers and users, to reveal the optimal strategies of each party in different situations, and to clarify the impact of information asymmetry, cost-benefit and other factors on decision-making. The results show that software vendors decide whether to disclose patches by weighing development costs against potential reputation losses; platforms determine whether to publicly disclose vulnerabilities based on their informational advantages and expected returns; hackers launch attacks by assessing the success rate of intrusions and potential gains; and users choose whether to apply fixes based on risk assessments of vulnerabilities. This paper provides a theoretical foundation for optimizing vulnerability disclosure mechanisms and enhancing information security management, and it holds significant implications for improving the overall information security governance system.

Keywords

Information Security, Sequential Game Theory, Vulnerability Disclosure, Information Asymmetry

1. 引言

信息科技的新技术不断推出，在享受新技术福利的同时，针对重要信息系统、基础应用和通用软硬件漏洞的攻击利用活跃，据第三方漏洞共享平台国家信息安全漏洞库平台(CNNVD)统计，近 3 年我国新增通用软/硬件漏洞的数量年均增长 20%左右，因漏洞引发的信息安全事故造成的经济损失超 1000 亿元，而 2017 年 CNVD 所披露的危急、高危、中危、低危漏洞对应的修复率分别仅为 88.46%、83.78%、75.14%、84.78%。这就不可避免地带来一个疑问，如果披露漏洞不能得到有效治理，漏洞信息披露岂不会带来更多的信息安全问题甚至成为某些黑客进行攻击的方向标？若平台公开披露周期过短，软件供应商漏洞补丁尚未开发完成，黑客利用披露信息可对该软件用户实施入侵；但若平台公开披露周期过长，则软件供应商漏洞补丁研发压力不足，黑客发现该漏洞并实施攻击的概率提升，不利于保护广大软件用户的利益。根据《中国互联网协会漏洞信息披露和处置自律公约》中提出适时披露原则，加强第三方漏洞共享平台、相关厂商和信息系统应用管理方的处置联动，针对不同漏洞的修复规律和所需周期，分析后确定灵活且实用的漏洞公开披露时间。因此，本文将采用序贯博弈方法研究第三方漏洞共享平台和各软件供应商之间的行为策略，分析研判第三方共享平台漏洞信息披露周期和软件供应商补丁披露周期等焦点问题。

2. 相关文献

信息安全漏洞的披露流程在第三方平台的运作下有序开展。当漏洞被发现后，发现者向平台递交漏洞信息，平台对其进行审核，审核通过后通知软件供应商。接着，软件供应商进行补丁开发，最后将开发好的补丁应用到相应的软件上，以此完成整个漏洞披露与修复的流程。网络安全漏洞披露已经成为网络安全风险控制的重要环节，对于降低风险和分化风险发挥着关键作用[1]。2002 年美国通过的《萨班斯法案》中的第 404 条要求上市公司每年必须出具一份自我披露漏洞的报告，该法案的实施促进了信息安

全漏洞知识的共享研究。Gordon 和 Loeb (2003)首先提出信息安全漏洞共享价值[2]。Cavusoglu 等(2007)、Ransbotham 等(2008)基于市场的漏洞披露机制的有效性，并将其与其他披露模式优缺点实施对比分析[3][4]。Gordon 等(2010)、Lei 等(2011)、Wang 等(2013)等进一步依据信息传递理论研究安全漏洞披露与企业市场价值之间的关系[5]-[7]。Tang 和 Whinston (2015)基于声誉机制设计了信息安全知识强制披露机制[8]。Mitra 和 Ransbotham (2015)则研究对比公开和半公开披露机制在信息安全知识共享过程中对黑客攻击行为产生的影响，并研究了两种披露机制下软件供应商和应用商各自的利弊[9]。Hausken (2017)重点阐述漏洞披露所带来的正效应及存在的负面影响[10]。国内在宏观层面上，学者尹建国(2013)、陈美(2014)、张涛等(2016)主要从国家战略、法律制度等理论层面，比较研究国内与美国、欧洲及韩国信息安全漏洞披露治理中的差异性[11]-[13]，指出协同多方主体的合作治理将是网络安全治理的重要议题[14]，微观层面上，有学者基于信息安全漏洞披露治理的关联性和复杂性，蒋鲁宁(2014)提出信息安全供应链概念[15]，并基于用户参与理论[16]、威慑论和制度理论[16]-[18]、面子倾向[19]、应对理论和道德推脱理论[20]等研究个体层面的信息安全漏洞治理。

漏洞披露共享已被证实为信息安全漏洞治理的有效方式，但多个主体之间如何建立合理的披露共享机制管控漏洞披露风险，即漏洞发现后何时披露的问题，变得越来越复杂和重要，且不同的漏洞披露策略，对软件用户、软件供应商、第三方漏洞共享平台等利益相关方造成的影响有很大不同。

3. 模型假设与构建

3.1. 模型假设

在当下的应用软件市场环境中，通常会出现这样的情况：有两家软件供应商，他们各自推出具备相似功能的应用软件。一旦这些软件中存在安全漏洞，且被黑客察觉，那么黑客便能够凭借该漏洞对所有存在类似问题的软件发起攻击，这无疑会给软件供应商和软件用户带来损失。

假定市场里的两家软件供应商 i，$i \in \{1,2\}$，在初始的 0 时刻，他们的软件进入市场，此时市场用户数量为 N_i。在 t_0 时刻，白帽子发现了软件中的漏洞，并把这一情况报告给第三方漏洞共享平台。平台收到信息后，会对漏洞的威胁程度进行评估与核实，之后通知相关软件供应商，同时确定平台向社会公开漏洞信息的时间周期(T)，这个周期对于整个漏洞处理流程至关重要。

软件供应商在得知漏洞信息后，需要考虑投入多少时间来开发补丁软件等安全补救措施，这一时间就是软件供应商漏洞补丁的披露周期，设其为 p_i。为便于研究，假设供应商 1 总是比供应商 2 更早披露漏洞补丁，即 $p_1 \le p_2$。接下来，本模型将从两种不同的情境展开深入研究，具体模型思路见图 1。

情境 A：软件供应商漏洞补丁在平台漏洞信息披露周期之前披露 $(t_o \le p_1 \le t_0 + T, p_2 \ge p_1)$；

情境 B：软件供应商漏洞补丁在平台漏洞信息披露周期之后披露 $(p_1 > t_0 + T, p_2 \ge p_1)$。

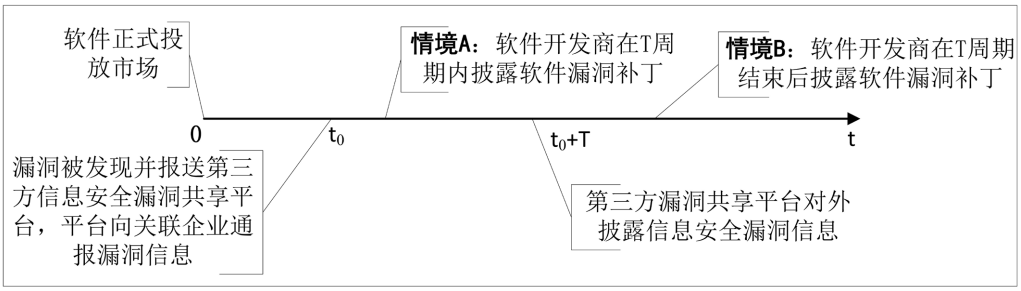

Figure 1. Model idea diagram
图 1. 模型思路图

3.2. 模型构建

(1) 模型相关参数

1) 软件供应商

① 补丁开发成本：软件供应商在处理漏洞时，其补丁开发成本用 $\varepsilon_{i1}-\varepsilon_{i2}(p-t)$ 来表示。这里的 ε_{i1} 是指软件补丁研发固定即时成本，也就是在开始研发补丁时就需要投入的成本； ε_{i2} 代表延迟研发可能为其带来的积极边际收益，在某些情况下，延迟研发虽然可能会使风险增加，但也可能带来诸如技术优化、成本降低等方面的收益。

② 黑客入侵相关参数：在漏洞信息尚未披露时，黑客发现软件漏洞的时间遵循概率密度为 α 的均匀分布，首次发现漏洞的时间记为 y。黑客对特定目标实施攻击的概率是 φ，软件被黑客成功入侵的概率为 δ。当第三方平台披露漏洞信息后，软件供应商 i 的用户被攻击的概率会上升至 $k\varphi$。如果一家软件供应商披露了漏洞补丁，而另一家未披露，那么未披露的软件供应商的用户被攻击概率会变为 $k^2\varphi$，其中 $k>1$。这是因为在信息不对称的情况下，未打补丁的软件更容易成为黑客的目标。

③ 风险防范与入侵概率变化：无论是第三方平台披露漏洞信息，还是软件供应商发布补丁之前，软件应用企业为降低风险，会采取一系列措施，比如关闭端口、权限升级以及关闭部分业务流程等。这些措施会使黑客成功入侵的概率降低，降低后的成功入侵概率设为 $\gamma\delta$， $\gamma\in(0,1)$。一旦软件应用企业获得补丁，就能完全抵御黑客的攻击。

④ 声誉损失：每次黑客成功攻击软件，都会给软件供应商带来声誉损失。假设每次成功攻击导致的声誉损失占比为 β，这部分损失会影响软件供应商的市场形象和未来的市场份额。

2) 第三方漏洞共享平台

第三方漏洞共享平台的期望是实现社会福利最大化或者社会损失最小化，其产生的社会成本主要涵盖以下几个方面：

① 软件供应商的补丁开发成本：这部分成本是平台需要考虑的重要因素之一，因为软件供应商为开发补丁投入的资源，间接影响着整个社会的资源分配和经济效率。

② 软件应用企业被攻击后的损失：例如金融等信息密集型行业一旦遭受攻击后，损失较大，而传统的劳动力密集型则相对较好。软件应用企业在遭受攻击后会遭受损失，其受损程度用 $N_iD\theta$ 来衡量。其中企业可能面临的最大损失金额用 D 表示，不同行业类型用 $\theta\sim U(0,1)$ 表示。例如金融等这类信息密集型行业，相比于传统的劳动力密集型行业，其在遭受攻击后，会产生更大的损失。

③ 软件应用企业的应对成本：当第三方平台披露漏洞信息后，软件应用企业为了应对风险，采取关闭端口、权限升级等措施，这会增加企业的成本。设单位时间内增加的成本为 s。这部分成本也构成了社会成本的一部分，需要平台在决策时予以考虑。

(2) 参与方决策函数

1) 软件供应商

在研究软件供应商的成本 V_{ij} 构成时，考虑到存在两种不同的情境，分别以 $j\in\{a,b\}$ 来表示。这两种情境下，软件供应商的成本主要涵盖了两个关键部分：一是研发成本，这是为开发漏洞补丁所投入的资源；二是在披露补丁前，由于黑客入侵而致使的声誉损失。

情境 A：软件供应商在平台披露周期之前披露漏洞补丁 $(t_0\le p_1\le t_0+T, p_2\ge p_1)$

$$V_{1a}=\varepsilon_{11}-\varepsilon_{12}(p_1-t_0)+N_1\beta\int_0^{p_1}\int_y^{p_1}\alpha\delta\varphi\mathrm{d}t\mathrm{d}y$$
$$V_{1a}=\varepsilon_{11}-\varepsilon_{12}(p_1-t_0)+\frac{N_1\beta\alpha\delta\varphi p_1^2}{2} \tag{1}$$

$$V_{2a}=\varepsilon_{21}-\varepsilon_{22}\left(p_2-t_0\right)+N_2\beta\left[\int_0^{p_1}\int_y^{p_1}\alpha\delta\varphi\mathrm{d}t\mathrm{d}y+\int_{p_1}^{p_2}\gamma\delta k^2\varphi\mathrm{d}t\right]$$
$$V_{2a}=\varepsilon_{21}-\varepsilon_{22}\left(p_2-t_0\right)+N_2\beta\left[\frac{\alpha\delta\varphi p_1^2}{2}+\gamma\delta k^2\varphi\left(p_2-p_1\right)\right] \tag{2}$$

情境 B：软件供应商在平台披露周期之后披露漏洞补丁 $\left(p_1>t_0+T,p_2\geq p_1\right)$

$$V_{1b}=\varepsilon_{11}-\varepsilon_{12}\left(p_1-t_0\right)+N_1\beta\left[\int_0^{t_0+T}\int_y^{t_0+T}\alpha\delta\varphi\mathrm{d}t\mathrm{d}y+\int_{t_0+T}^{p_1}\gamma\delta k\varphi\mathrm{d}t\right]$$
$$V_{1b}=\varepsilon_{11}-\varepsilon_{12}\left(p_1-t_0\right)+N_1\beta\left[\frac{\alpha\delta\varphi\left(t_0+T\right)^2}{2}+\gamma\delta k\varphi\left(p_1-t_0-T\right)\right] \tag{3}$$

$$V_{2b}=\varepsilon_{21}-\varepsilon_{22}\left(p_2-t_0\right)+N_2\beta\left[\int_0^{t_0+T}\int_y^{t_0+T}\alpha\delta\theta\mathrm{d}t\mathrm{d}y+\int_{t_0+T}^{p_1}\gamma\delta k\varphi\mathrm{d}t+\int_{p_1}^{p_2}\gamma\delta k^2\varphi\mathrm{d}t\right]$$
$$V_{2b}=\varepsilon_{21}-\varepsilon_{22}\left(p_2-t_0\right)+N_2\beta\left[\frac{\alpha\delta\varphi\left(t_0+T\right)^2}{2}+\gamma\delta k\varphi\left(p_1-t_0-T\right)+\gamma\delta k^2\varphi\left(p_2-p_1\right)\right] \tag{4}$$

2) 第三方漏洞共享平台

漏洞共享平台的成本 C_i 是由多个关键部分构成。首先，软件供应商的总研发成本是重要组成部分之一，它涵盖了从发现漏洞到开发出补丁这一过程中，软件供应商投入的所有资源，包括人力、物力和时间成本等。其次，软件用户因黑客入侵而产生的损失同样不可忽视。一旦黑客利用软件漏洞成功入侵，软件用户可能面临数据泄露、业务中断、财产损失等多种问题。最后，部分用户在补丁未披露前关闭软件部分功能所产生的损失也是成本的一部分。当用户得知软件存在漏洞且补丁尚未发布时，为了降低风险，他们可能会主动关闭软件的某些功能，这一行为虽然在一定程度上减少了潜在的安全风险，但也会导致用户体验下降，甚至可能影响软件的正常使用。

情境 A：软件供应商在平台披露周期之前披露漏洞补丁 $\left(t_0\leq p_1\leq t_0+T,p_2\geq p_1\right)$

$$C_a=\varepsilon_{11}-\varepsilon_{12}\left(p_1-t_0\right)+\varepsilon_{21}-\varepsilon_{22}\left(p_2-t_0\right)+\left(N_1+N_2\right)\int_0^{p_1}\int_y^{p_1}\int_0^1\alpha\delta\varphi\theta D\mathrm{d}\theta\mathrm{d}t\mathrm{d}y$$
$$+\int_{p_1}^{p_2}\int_0^1N_2\gamma\delta k^2\varphi D\theta\mathrm{d}\theta\mathrm{d}t+\int_{p_1}^{p_2}N_2\mathrm{s}\mathrm{d}t$$
$$C_a=\left(\varepsilon_{11}+\varepsilon_{21}\right)-\varepsilon_{12}\left(p_1-t_0\right)-\varepsilon_{22}\left(p_2-t_0\right)+\left(N_1+N_2\right)\frac{\alpha\delta\varphi D}{4}p_1^2$$
$$+N_2\left(p_2-p_1\right)\left(\frac{\gamma\delta\varphi k^2D}{2}+s\right) \tag{5}$$

情境 B：软件供应商在平台披露周期之后披露漏洞补丁 $\left(p_1>t_0+T,p_2\geq p_1\right)$

$$C_b=\varepsilon_{11}-\varepsilon_{12}\left(p_1-t_0\right)+\varepsilon_{21}-\varepsilon_{22}\left(p_2-t_0\right)+\left(N_1+N_2\right)\int_0^{t_0+T}\int_y^{t_0+T}\int_0^1\alpha\delta\varphi\theta D\mathrm{d}\theta\mathrm{d}t\mathrm{d}y$$
$$+\left(N_1+N_2\right)\int_{t_0+T}^{p_1}\int_0^1\gamma\delta k\varphi D\theta\mathrm{d}\theta\mathrm{d}t+\left(N_1+N_2\right)\int_{t_0+T}^{p_1}\mathrm{s}\mathrm{d}t+N_2\int_{p_1}^{p_2}\int_0^1\gamma\delta k\varphi D\theta\mathrm{d}\theta\mathrm{d}t+N_2\int_{p_1}^{p_2}\mathrm{s}\mathrm{d}t$$
$$C_b=\left(\varepsilon_{11}+\varepsilon_{21}\right)-\varepsilon_{12}\left(p_1-t_0\right)-\varepsilon_{22}\left(p_2-t_0\right)+\left(N_1+N_2\right)D\frac{\alpha\delta\varphi\left(t_0+T\right)^2}{4}$$
$$+N_1\left(p_1-t_0-T\right)\left(D\frac{\gamma\delta k\varphi}{2}+s\right)+N_2\left(p_2-t_0-T\right)\left(D\frac{\gamma\delta k\varphi}{2}+s\right) \tag{6}$$

4. 模型分析

4.1. 软件供应商漏洞补丁披露策略分析

(1) 情境 A：软件供应商在平台披露周期之前披露漏洞补丁 $\left(t_0 \le p_1 \le t_0+T, p_2 \ge p_1\right)$

在两家软件供应商博弈过程中，假定软件供应商 1 为市场先行者，因此对式(2)求导，求解得出软件供应商 2 的最优策略为：

$$p_{2a}^{*}=\begin{cases} p_{1a} & \beta N_2\gamma\delta k^2\varphi \ge \varepsilon_{22} \\ \infty & \beta N_2\gamma\delta k^2\varphi < \varepsilon_{22} \end{cases}$$

对式(1)求导，求解得出软件供应商 1 的最优策略为：

$$p_{1a}^{*}=\begin{cases} t_0 & t_0 > \dfrac{\varepsilon_{12}}{N_1\alpha\beta\delta\varphi} \\ \dfrac{\varepsilon_{12}}{N_1\alpha\beta\delta\varphi} & t_0 \le \dfrac{\varepsilon_{12}}{N_1\alpha\beta\delta\varphi} \le t_0+T \\ t_0+T & \dfrac{\varepsilon_{12}}{N_1\alpha\beta\delta\varphi} > t_0+T \end{cases}$$

令 $\phi_1=\dfrac{\varepsilon_{12}}{N_1\beta\delta\varphi}$ 表示软件供应商 1 单位时间成本收益率，$\phi_2=\dfrac{\varepsilon_{22}}{N_2\beta\delta\varphi}$ 软件供应商 2 单位时间成本收益率。

情境 A 下供应商策略矩阵见表 1。

Table 1. Supplier strategy matrix under Scenario A
表 1. 情境 A 下供应商策略矩阵

条件	p_{1a}^{*}	p_{2a}^{*}	
		$\gamma k^2 \ge \phi_2$	$\gamma k^2 < \phi_2$
$t_0 > \phi_1/\alpha$	t_0	t_0	∞
$t_0 \le \phi_1/\alpha \le t_0+T$	ϕ_1/α	ϕ_2/α	∞
$\phi_1/\alpha > t_0+T$	t_0+T	t_0+T	∞

Table 2. Supplier strategy matrix under Scenario B
表 2. 情境 B 下供应商策略矩阵

条 件	p_{1b}^{*}	p_{2b}^{*}	
		$\gamma k^2 \ge \phi_2$	$\gamma k^2 < \phi_2$
$\gamma k \ge \phi_1$	t_0+T	t_0+T	∞
$\gamma k < \phi_1$	∞	∞	∞

(2) 情境 B：软件供应商在平台披露周期之后披露漏洞补丁 $\left(p_1 > t_0+T, p_2 \ge p_1\right)$

对式(4)求导，求解得出软件供应商 2 的最优策略为：

$$p_{b2}^{*}=\begin{cases} p_{b1} & \beta N_2\gamma\delta k^2\varphi \ge \varepsilon_{22} \\ \infty & \beta N_2\gamma\delta k^2\varphi < \varepsilon_{22} \end{cases}$$

对式(3)求导，求解得出软件供应商 1 的最优策略为：

$$p_{b1}^{*}=\begin{cases}t_0+T & N_1\beta\gamma\delta k\varphi\geq\varepsilon_{12}\\ \infty & N_1\beta\gamma\delta k\varphi<\varepsilon_{12}\end{cases}$$

情境 B 下供应商策略矩阵见表 2。

4.2. 第三方漏洞共享平台信息披露策略

(1) 假设 $\gamma k\geq\phi_1$， $\gamma k^2\geq\phi_2$ 条件均成立

从表 1 与表 2 所呈现的数据及分析结果能够看出，在特定条件下，即当 $t_0>\phi_1/\alpha$ 满足时，软件供应商针对漏洞补丁的披露策略会表现为即时披露 $p_i^{*}=t_0$。具体而言，软件供应商会选择在第一时间发布补丁，此时其决策并不受第三方平台漏洞信息披露周期 T 的影响。也就是说，无论第三方平台何时披露漏洞信息，软件供应商都决定立刻采取行动，推出补丁以修复漏洞。在这种情况下，对于第三方平台而言，其策略选择相对较为灵活，T 的取值可以是任意的。

当 $t_0\leq\phi_1/\alpha\leq t_0+T$ 时， $p_1=\phi_1/\alpha$， $p_2=\phi_2/\alpha$，此时第三方平台的成本与披露周期相互独立，因此 $T^{*}\in\left[\phi_1/\alpha-t_0,\infty\right]$。

当 $\phi_1/\alpha>t_0+T$ 时，将 $p_1^{*}=t_0+T$， $p_2^{*}=t_0+T$ 代入式(5)后，对 T 求导得：

$$T^{*}=\begin{cases}0 & \omega_1<t_0\\ \omega_1-t_0 & t_0<\omega_1<\phi_1/\alpha\\ \phi_1/\alpha-t_0 & \omega_1>\phi_1/\alpha\end{cases}$$

其中 $\omega_1=\dfrac{2\left(\varepsilon_{12}+\varepsilon_{22}\right)}{\left(N_1+N_2\right)\alpha\delta\varphi\theta D}$。

(2) 假设 $\gamma k\geq\phi_1$， $\gamma k^2<\phi_2$ 条件均成立

将 $p_{2a}^{*}=\infty$ 代入式(5)后得：

$$C_a=\left(\varepsilon_{11}+\varepsilon_{21}\right)-\varepsilon_{12}\left(p_1-t_0\right)-\varepsilon_{22}\left(p_2-t_0\right)+\left(N_1+N_2\right)\frac{\alpha\delta\varphi\theta D}{4}p_1^2$$
$$+N_2\left(p_2-p_1\right)\left(\frac{\theta\gamma\delta\varphi k^2D}{2}+s\right)$$

在特定的情形下，即当 $t_0>\phi_1/\alpha$ 满足时，软件供应商便会无一例外地选择即时披露漏洞补丁，$p_1^{*}=t_0$。在这一决策过程中，软件供应商的行为表现为，他们在决定披露补丁的时间节点时，并不会将第三方平台的漏洞公开周期 T 纳入考量范围。在这种状况下，第三方平台在漏洞披露策略上拥有较大的自主性，其策略变量 T 取值不受软件供应商决策的限制，可以根据多种因素灵活确定。

当 $t_0\leq\phi_1/\alpha\leq t_0+T$ 时， $p_1=\phi_1/\alpha$， $p_2=\infty$，此时第三方平台的成本与披露周期相互独立，因此 $T^{*}\in\left[\phi_1/\alpha-t_0,\infty\right]$。

当 $\phi_1/\alpha>t_0+T$ 时，

$$T^{*}=\begin{cases}0 & \omega_2<t_0\\ \omega_2-t_0 & t_0<\omega_2<\phi_1/\alpha\\ \phi_1/\alpha-t_0 & \omega_2>\phi_1/\alpha\end{cases}$$

其中令 $\omega_2=\dfrac{2\varepsilon_{12}+N_2\delta\theta\varphi\gamma k^2D+2N_2s}{\left(N_1+N_2\right)\alpha\delta\varphi\theta D}$。

(3) 在某些特定情况下，即当 $\gamma k<\phi_1$ 满足时，软件供应商会出现一种决策倾向，即无论第三方平台的漏洞披露周期怎样变动，他们都可能选择不发布信息安全漏洞补丁。然而，如果平台也选择不披露这

类漏洞信息，也就是当$T=\infty$，意味着永远不公开相关漏洞信息时，情境 B 所设定的条件$\left(p_1 \geq t_0+T\right)$)将无法成立。在这种特殊状况下，借助公式(1)对软件供应商 1 的决策进行分析求解，可以得出其最优策略为：$p_1^*=\max\left\{t_0,\phi_1/\alpha\right\}$。

软件供应商 2 的最优策略为：

$$p_1^*=\begin{cases}\max\left\{t_0,\phi_1/\alpha\right\} & \beta N_2\gamma\delta k^2\varphi \geq \varepsilon_{22}\\ \infty & \beta N_2\gamma\delta k^2\varphi < \varepsilon_{22}\end{cases}$$

综上分析，博弈各参与方在各种条件下的策略汇总如表 3 所示：

Table 3. Strategy matrix for each participant of the game
表 3. 博弈各参与方策略矩阵

应用条件	第三方漏洞共享平台 T^*	软件供应商 p_1^*	软件供应商 p_2^*
$\gamma k<\phi_1$ $\gamma k^2\geq\phi_2$	∞	$\max\left\{t_0,\phi_1/\alpha\right\}$	$\max\left\{t_0,\phi_1/\alpha\right\}$
$\gamma k<\phi_1$ $\gamma k^2<\phi_2$	∞	$\max\left\{t_0,\phi_1/\alpha\right\}$	∞
$\gamma k\geq\phi_1,\gamma k^2\geq\phi_2$ $t_0>\phi_1/\alpha$	任意值	t_0	t_0
$\gamma k\geq\phi_1,\gamma k^2\geq\phi_2$ $t_0\leq\phi_1/\alpha\leq t_0+T$	$\left[\phi_1/\alpha-t_0,\infty\right]$	ϕ_1/α	ϕ_2/α
$\gamma k\geq\phi_1,\gamma k^2\geq\phi_2$ $\phi_1/\alpha>t_0+T$ $\omega_1<t_0$	0	t_0+T	t_0+T
$\gamma k\geq\phi_1,\gamma k^2\geq\phi_2$ $\phi_1/\alpha>t_0+T$ $t_0<\omega_1<\phi_1/\alpha$	ω_1-t_0	t_0+T	t_0+T
$\gamma k\geq\phi_1,\gamma k^2\geq\phi_2$ $\phi_1/\alpha>t_0+T$ $\omega_1>\phi_1/\alpha$	$\phi_1/\alpha-t_0$	t_0+T	t_0+T
$\gamma k\geq\phi_1,\gamma k^2<\phi_2$ $t_0>\phi_1/\alpha$	任意值	t_0	∞
$\gamma k\geq\phi_1,\gamma k^2<\phi_2$ $t_0\leq\phi_1/\alpha\leq t_0+T$	$\left[\phi_1/\alpha-t_0,\infty\right]$	ϕ_1/α	∞
$\gamma k\geq\phi_1,\gamma k^2<\phi_2$ $\omega_2<t_0$	0	t_0+T	∞
$\gamma k\geq\phi_1,\gamma k^2<\phi_2$ $t_0<\omega_2<\phi_1/\alpha$	ω_2-t_0	t_0+T	∞
$\gamma k\geq\phi_1,\gamma k^2<\phi_2$ $\omega_2>\phi_1/\alpha$	$\phi_1/\alpha-t_0$	t_0+T	∞

5. 结论

在第三方信息安全漏洞共享平台的生态体系中，不同参与主体各自遵循着不同的行为决策规则。其中，作为关键第三方介入角色的共享平台，如果在信息安全知识的披露范围界定、披露时序安排等方面存在缺陷，不仅无法有效防控安全风险，反而可能促使安全风险进一步扩散。

为了深入研究这一复杂现象，本文构建了多种情境，以实现社会福利最大化为核心目标，深入分析第三方漏洞平台与软件供应商在安全漏洞披露中的行为博弈。在整个信息安全漏洞处理流程里，软件供应商作为核心主体之一，对漏洞的容忍程度存在显著差异。其信息安全漏洞补丁的披露周期并非固定不变，而是受到诸多因素的综合制约。例如，市场占有率(N_i)会影响软件供应商的决策，市场占有率较高的供应商可能更注重维护品牌形象，从而更积极地应对漏洞披露；漏洞补丁开发时间成本收益率(ϕ_i)也至关重要，若开发成本过高且收益不明显，供应商可能会延迟补丁披露；黑客的攻击能力(φ、δ、γ、k)同样不可忽视，强大的攻击能力会给软件供应商带来更大的压力，影响其披露决策；此外，漏洞初始发现时刻(t_0)也会对软件供应商的决策产生影响，较早发现的漏洞可能会让供应商有更充裕的时间来准备补丁披露。作为第三方漏洞信息共享平台为了社会福利最大化需要综合考虑市场参与者的反应来制定漏洞信息披露周期，平衡“公众被告知相关安全漏洞”与“生产商具有充分的时间进行有效的回应”之间的矛盾。本文通过建模分析为第三方漏洞共享平台和软件供应商构建了一个基于社会福利最优化的信息安全漏洞披露周期时间表，为各参与方就信息漏洞披露决策提供了借鉴。

参考文献

[1] 黄道丽. 网络安全漏洞披露规则及其体系设计[J]. 暨南学报(哲学社会科学版), 2018(1): 94-106.

[2] Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003) Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy*, **22**, 461-485. https://doi.org/10.1016/j.jaccpubpol.2003.09.001

[3] Ransbotham, S., Mitra, S. and Ramsey, J. (2012) Are Markets for Vulnerabilities Effective? *MIS Quarterly*, **36**, 43-64. https://doi.org/10.2307/41410405

[4] Cavusoglu, H., Cavusoglu, H. and Raghunathan, S. (2007) Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge. *IEEE Transactions on Software Engineering*, **33**, 171-185. https://doi.org/10.1109/tse.2007.26

[5] Gordon, L.A., Loeb, M.P. and Sohail, T. (2010) Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, **34**, 567-594. https://doi.org/10.2307/25750692

[6] Lei, M., Zhou, S.L., Yang, X.X., *et al*. (2012) The Consequences of Information Technology Control Weaknesses on Management Information Systems: The Case of Sarbanes-Oxley Internal Control Reports. *MIS Quarterly*, **36**, 179-203. https://doi.org/10.2307/41410413

[7] Wang, T., Kannan, K.N. and Ulmer, J.R. (2013) The Association between the Disclosure and the Realization of Information Security Risk Factors. I*nformation Systems Research*, **24**, 201-218. https://doi.org/10.1287/isre.1120.0437

[8] Tang, Q. and Whinston, A.B. (2015) Improving Internet Security through Mandatory Information Disclosure. 2015 48*th Hawaii International Conference on System Sciences*, Kauai, 5-8 January 2015, 4813-4823. https://doi.org/10.1109/hicss.2015.572

[9] Mitra, S. and Ransbotham, S. (2015) Information Disclosure and the Diffusion of Information Security Attacks. *Information Systems Research*, **26**, 565-584. https://doi.org/10.1287/isre.2015.0587

[10] Hausken, K. (2017) Security Investment, Hacking, and Information Sharing between Firms and between Hackers. *Games*, **8**, 1-23. https://doi.org/10.3390/g8020023

[11] 尹建国. 美国网络信息安全治理机制及其对我国之启示[J]. 法商研究, 2013, 30(2): 138-146.

[12] 陈美. 国家信息安全协同治理: 美国的经验与启示[J]. 情报杂志, 2014, 33(2): 10-14.

[13] 张涛, 王玥, 黄道丽. 信息系统安全治理框架: 欧盟的经验与启示——基于网络攻击的视角[J]. 情报杂志, 2016, 35(8): 17-24.

[14] 董俊祺. 韩国网络空间的主体博弈对我国信息安全治理的启示——以韩国网络实名制政策为例[J]. 情报科学,

2016, 34(4): 153-157.

[15] 蒋鲁宁. 信息安全供应链的安全[J]. 中国信息安全, 2014(3): 111.

[16] 谢宗晓, 林润辉, 王兴起. 用户参与对信息安全管理有效性的影响——多重中介方法[J]. 管理科学, 2013, 26(3): 65-76.

[17] 林润辉, 谢宗晓, 王兴起, 等. 制度压力、信息安全合法化与组织绩效——基于中国企业的实证研究[J]. 管理世界, 2016, 32(2): 112-127.

[18] 甄杰, 谢宗晓, 林润辉. 治理机制、制度化与企业信息安全绩效[J]. 工业工程与管理, 2018, 23(3): 171-176.

[19] 陈昊, 李文立, 陈立荣. 组织控制与信息安全制度遵守: 面子倾向的调节效应[J]. 管理科学, 2016, 29(3): 1-12.

[20] 甄杰, 谢宗晓, 董坤祥. 信息安全压力与员工违规意愿: 被调节的中介效应[J]. 管理科学, 2018, 31(4): 91-102.