本专著受国家自然科学基金（项目号71801125）、
江苏省社会科学基金（项目号17GLD008）资助

The Management Strategy of
Information Systems Security Technology:
An Information Security Economics Perspective

信息系统安全技术管理策略：
信息安全经济学视角

赵柳榕／著

西南财经大学出版社

本专著受国家自然科学基金（项目号71801125）、
江苏省社会科学基金（项目号17GLD008）资助

信息系统安全技术管理策略：
信息安全经济学视角

赵柳榕／著

The Management Strategy of
Information Systems Security Technology:
An Information Security Economics Perspective

西南财经大学出版社
·成都·

图书在版编目(CIP)数据

信息系统安全技术管理策略:信息安全经济学视角/赵柳榕著. —成都:
西南财经大学出版社,2020.3
ISBN 978-7-5504-0704-6

Ⅰ.①信… Ⅱ.①赵… Ⅲ.①信息系统—安全管理 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字(2018)第 276547 号

信息系统安全技术管理策略:信息安全经济学视角

XINXI XITONG ANQUAN JISHU GUANLI CELÜE: XINXI ANQUAN JINGJIXUE SHIJIAO

赵柳榕 著

策划编辑:何春梅
责任编辑:何春梅
封面设计:墨创文化
责任印制:朱曼丽

出版发行	西南财经大学出版社(四川省成都市光华村街 55 号)
网　　址	http://www.bookcj.com
电子邮件	bookcj@foxmail.com
邮政编码	610074
电　　话	028-87353785
照　　排	四川胜翔数码印务设计有限公司
印　　刷	四川新财印务有限公司
成品尺寸	170mm×240mm
印　　张	14.5
字　　数	215 千字
版　　次	2020 年 3 月第 1 版
印　　次	2020 年 3 月第 1 次印刷
书　　号	ISBN 978-7-5504-0704-6
定　　价	88.00 元

前 言

随着互联网的普及和信息化建设的不断推进，信息系统已经成为组织赖以生存的重要资源，信息系统安全问题是关系到企业持续稳健发展、社会长治久安的重大战略问题。与此同时，各类接入互联网的信息系统受到的安全威胁越来越大，黑客攻击水平越来越高，信息安全问题给各行业组织造成了声誉和财务上的巨大损失。面对日趋严峻的信息安全形势，很多企业组合运用防火墙、入侵检测（IDS）、漏洞扫描、防病毒软件、蜜罐技术、虚拟专用网（VPN）等多种安全防御技术和安全检测技术提升信息系统安全水平。然而，现行有关信息安全问题的研究主要侧重于安全技术算法的开发和优化，而较少考虑系统安全性、经济性和保障系统正常运行之间的平衡，这就给传统的信息安全研究提出了挑战。为此，信息系统管理专业出现了一个新的研究领域——信息安全经济学，主要研究信息安全的投资—效益形式和条件、黑客攻击行为对企业或社会经济产生影响的规律、信息安全技术的效果和效益等问题。本书基于信息安全经济学视角，综合应用博弈论、决策理论和概率论等多种理论和方法，对企业信息系统安全技术运用策略和管理的相关问题进行了研究。

首先，本书介绍了信息系统安全技术的研究背景和意义，梳理了近年来的全球信息安全大事件。通过分析信息系统安全需求的演变过程，我们发现影响信息系统安全的不只是技术问题，人的决策因素也影响着整个信息系统的安全性。本书结合我国 2017 年实施的《中华人民共和国网络安全法》的相关要求，指出无论是基于企业的需求还是国家的强制要求，将

技术开发和经济管理理论相结合进行研究已成为信息系统安全领域中的关键任务，应用严谨的理论方法体系科学地解决信息系统安全问题已迫在眉睫。同时本书还阐明了合理制定信息系统安全技术组合策略的理论意义和实践意义。

其次，为了更好地理解并应用信息安全经济学理论，本书基于著名的WEIS会议上相关学者的成果，分析信息安全经济学的发展脉络和热点问题，总结了目前该领域重点关注和亟需解决的相关问题，包括信息系统安全市场与环境问题、信息系统安全风险问题、信息系统安全技术投资问题等，特别是信息系统安全技术管理的相关研究。接下来，基于已有的文献和权威组织机构的定义定义了信息系统安全技术和纵深防御的相关概念，总结了信息安全技术及其组合的原理和特点，梳理了信息系统安全策略的制定过程，探讨了制定安全策略需要考虑的主要因素。这两部分内容从理论和应用角度总结了相关问题和研究方法，是本书后续内容的分析基础。

再次，由于网络攻击的种类繁多且情况复杂程度越来越高，没有一种信息安全技术可以完全应对信息系统的内外部威胁，因此组合运用多种安全技术保护信息系统已成为各企业信息系统安全技术管理策略的首选方案。本书基于博弈论、决策理论等相关知识，研究了两种主流信息安全技术组合的最优配置策略，分别建立了蜜罐和入侵检测系统（IDS）、虚拟专用网和入侵检测系统的数学模型，将企业、黑客、信息安全技术的影响参数和决策变量纳入模型，定量刻画并分析了企业两种信息系统安全技术组合的管理模型。本书还分析了配置一种信息安全技术和同时配置两种技术组合的纳什均衡混合策略，研究了两种信息安全技术组合的技术参数对黑客最优入侵策略的影响。研究结果表明，两种信息安全技术组合并不一定总是最优配置策略。当企业的安全目标是使黑客入侵概率降低到一定值时，我们可以通过定量计算得到配置蜜罐和IDS技术组合的预算范围；配置虚拟专用网与降低入侵检测系统的误报率并不总是正相关的。

进一步地，本书研究了三种信息安全技术组合最优配置策略，并对其技术交互进行了经济学分析。在复杂的网络环境和严格的安全需求下，保证信息系统的动态安全往往需要配置两种以上的信息安全技术。例如，企

业面临基于攻击检测的综合联动控制问题时，往往需要通过采用配置防火墙、IDS 和漏洞扫描的技术组合方案来解决。本书从技术原理角度定性分析了这三种技术组合的信息安全模型，通过引入企业、黑客、信息安全技术的影响参数和决策变量对三种技术组合的信息安全模型进行定量刻画，同时，通过分别求解企业只配置 IDS 和漏洞扫描技术以及配置防火墙、IDS 和漏洞扫描技术的纳什均衡解和均衡条件来分析了三种信息安全技术组合的最优配置策略。结合“信息安全金三角模型”，我们从经济学角度定义了不同信息安全技术存在互补或冲突。研究结果表明，被修复的漏洞并非越多越好，只有在特定情况下，配置漏洞扫描技术才会对系统带来正的效应，得到三种技术冲突与互补的条件。

另外，人的行为特征也是影响信息系统安全技术管理决策的重要因素。无论是企业还是黑客，其行为都要承担相应的风险，我们认为，博弈过程中利益相关者的风险偏好属性值得深入探究。因此，本书以主流的信息安全技术组合为例，研究了基于风险偏好的防火墙和入侵检测的最优配置策略。除了企业、黑客、信息安全技术的参数和决策变量外，在博弈模型中还引入了包含利益相关者风险偏好的参数，分别分析了在只配置 IDS、只配置防火墙以及同时配置 IDS 和防火墙三种配置策略下，黑客的最优入侵策略和企业风险偏好之间的关系、企业的人工调查策略和黑客风险偏好之间的关系。我们定量研究了信息安全技术对信息系统的防御和检测的经济效用，讨论了已配置了 IDS 或防火墙的企业需要增加配置防火墙或 IDS 技术的条件，以及当企业的预算只能支持一种安全技术时应如何决策。研究结果表明，当企业的期望成本较低时，风险中立型企业更易被入侵；当企业的期望成本较高时，风险厌恶型企业更易被入侵。当黑客的期望收益较低时，风险厌恶型黑客被检测的概率最大；当黑客的期望收益较高时，风险追求型黑客被检测的概率最大。

最后，信息系统安全管理人员和黑客在博弈时无法做到完全理性，也很难完全正确预测对方的行为，因此有必要分析有限理性的利益相关者决策。本书基于演化博弈理论研究了防火墙和入侵检测系统的配置策略。为了和前面的研究内容进行比较，同样研究了只配置 IDS、只配置防火墙以

及同时配置IDS和防火墙三种信息安全技术组合配置策略。通过分析利益相关者的演化博弈收益矩阵，求解复制动态的稳定状态，讨论了稳定状态的邻域稳定性，分析了影响双方演化稳定策略的条件，以及影响各个模型的演化稳定策略阈值的因素。结果表明，当企业只配置入侵检测系统且IDS报警时，较高的入侵检测概率使黑客入侵概率大大降低，较低的入侵概率使企业采用人工调查的概率大大降低。当企业只配置防火墙且报警时，系统的演化稳定状态为黑客不入侵系统、企业不采取人工调查；当防火墙不报警时，较高的防火墙检测概率降低人工调查概率的程度大于较高的IDS检测概率降低人工调查概率的程度；较低的防火墙检测概率降低入侵概率的程度大于较低的IDS检测概率降低入侵概率的程度。当企业配置这两种技术组合且联动检测概率大于IDS入侵检测概率时，系统的演化稳定状态为企业配置两种信息安全联动技术、黑客不入侵系统；否则，系统的演化稳定状态则为企业应只配置IDS技术、黑客入侵系统。

本书得到了国家自然科学基金（项目号71801125）、江苏省社会科学基金（项目号17GLD008）的资助。笔者在撰写本书的过程中，得益于笔者博士生阶段的导师、东南大学梅姝娥教授的悉心指导，以及课题组的仲伟俊教授、硕士生阶段的导师田立新教授、博士后阶段的导师肖条军教授的宝贵意见。感谢东南大学经济管理学院的高星副教授，扬州大学商学院的顾建强博士和方玲博士，江苏大学管理学院的熊强副教授，南京工业大学经济与管理学院的张琳教授，陆敬筠教授和朱晓峰教授的帮助！最后，特别感谢我的父母对我的辛勤培育和无条件的支持！感谢我的丈夫对我无微不至的呵护和温暖的鼓励！

赵柳榕

2019年12月

目 录

1 绪论

随着我国“互联网+”战略的积极推进，信息化大潮汹涌而至，无论是互联网企业还是传统企业都越来越依赖网络方式获得信息和交流信息，信息系统对企业的日常运行和管理、提高生产运营效率等都起着至关重要的作用。然而，企业在享受信息技术带来的便利和效益同时，其网络环境和技术的复杂性也使得保护信息资产和信息系统面临前所未有的挑战。

目前，各类接入互联网的信息系统受到的安全威胁越来越大，黑客攻击水平越来越高，信息安全问题日益突出，给各行业组织带来声誉和财务上巨大的损失。例如，2017 年 5 月永恒之蓝勒索病毒波及 150 个国家的高校、政府机构、国有企业等，造成的损失超 80 亿美元。根据世界经济论坛发布的《2017 年全球风险报告》，大规模网络安全破坏位居当今世界面临的五大最严重风险之列。在我国，网络安全问题已经上升到了国家安全层面，企业对信息安全的重视也达到了前所未有的高度，并通过购买最新的信息安全技术、引进信息安全人才积极来应对各类威胁。然而，安全技术虽然可以在一定程度上保障信息系统，但其技术本身也存在着潜在的漏洞和风险。黑客不仅利用技术弱点攻击单个计算机系统，还利用网络连接的特性攻击和它相连的电脑。一些实证和理论研究表明，越来越多的黑客入侵是有目的的，但他们做出攻击的决策也取决于系统的安全性。面对严峻的信息系统安全形势，组合运用防火墙、入侵检测（IDS）、防病毒、安全日志、人工调查、加密、数据备份等多种安全技术提升信息系统安全水平，已经成为信息系统应用中的关键问题之一。此外，企业的信息安全预

算已经成为其资本结构的重要组成部分，如何在有限的资金条件下达到最优的信息系统安全技术管理水平也是企业和学术界关注的热点问题。

1.1 信息系统安全技术研究背景和意义

1.1.1 信息系统安全技术研究背景

信息技术的进步引发了经济社会的深刻变革，社会正在被“再结构”，人类正在迈入一个全新的时代。各种技术风起云涌，终端设备在进化、数据中心在进化、数字威胁也在进化中，如果信息系统打开了“漏洞”的缺口，则一切的资产、核心竞争力、信誉等支撑组织运行的重要因素将消失瓦解。信息系统的安全已成为影响经济社会发展和稳定的重要因素之一。早在2014年我国就成立了中央网络安全和信息化领导小组，由习近平总书记担任组长，李克强总理和刘云山担任副组长，其功能为统筹协调各个领域的网络安全和信息化的重大问题，制定和实施国家网络安全和信息化发展战略、宏观规划和重大政策，不断增强安全保障能力。在第一次会议上，习近平总书记就指出，网络安全和信息化对一个国家很多领域都是牵一发而动全身，需要推进国家网络安全战略，加强网络安全能力建设。近年来，全球发生的重大信息安全事件风险成因复杂，既有外部攻击，也有内部泄露，既有技术漏洞，也有管理缺陷；既有新技术新模式触发的新风险，也有传统安全问题的持续触发。一旦发生信息安全事故，其影响都将超越技术范畴和组织边界，对经济、政治和社会等领域产生影响，包括产生重大财产损失、威胁生命安全和改变政治进程。

2013年6月爆发的“棱镜门”事件引起了轩然大波，凸显了全球网络安全的重要性。斯诺登爆料：美国国家安全局曾入侵中国移动公司以获取手机的短信信息，并持续攻击清华大学的主干网络以及电信企业Pacnet香港总部的计算机。也就是说，美国国家安全局可以侵入众多国家的网络终

端领域进行大规模的窃听和监视全球所有人的个人隐私，从而掌握重要的一线情报资料。

2014 年 2 月，全球最大的比特币交易平台 Mt. Gox 由于交易系统出现漏洞，75 万个比特币以及 Mt. Gox 自身账号中约 10 万个比特币被窃，损失估计达到 4.67 亿美元，被迫宣布破产。同年 4 月出现的 Heartbleed 漏洞是近年来涉及各大网银、门户网站等影响范围最广的高危漏洞。该漏洞可被用于窃取服务器敏感信息，实时抓取用户的账号和密码。预计即使是在今后十年中，仍会在成千上万台服务器上发现这一漏洞，甚至包括一些非常重要的服务器。

2015 年 2 月，由于没有设置额外的认证机制，美国第二大医疗保险公司 Anthem 被黑客入侵并盗走 8 000 万份个人信息，医疗机构成为信息泄露的重灾区。黑客可以成功入侵系统的原因不仅是缺少数据加密，还有不正确的访问控制机制。这些都是基于业务和运营需要所做的系统及访问控制，需要重点考虑安全策略问题。2015 年 8 月，英国电信运营商 Carphone Warehouse 约 240 万在线用户的个人信息遭到黑客入侵，其中包括姓名、地址、出生日期和银行卡信息等，多达 9 万名客户的加密信用卡数据可能也遭到了黑客的入侵。由于未恰当使用和配置数据库防火墙系统对外部黑客攻击进行防御，这些数据的批量泄漏会导致一系列电信诈骗的发生并致使电信运营商信誉受损。

2016 年 9 月，雅虎先后证实共超过 15 亿用户信息遭窃，其被认为是互联网史上最大规模的信息安全泄露事件。泄露原因是近年来雅虎只偏重业务发展而忽视了安全问题，此次事故对 Verizon 公司收购雅虎的交易产生了重大影响。

2017 年 5 月，勒索病毒 WannaCry 在全球范围内爆发，这场全球最大范围的网络攻击已经造成至少 150 个国家的 20 万台电脑受到感染，受害者包括中国、英国、俄罗斯、德国和西班牙等国的医院、大学、制造商和政府机构。同年 11 月，美国五角大楼意外暴露了美国国防部的分类数据库，其中包含美国当局在全球社交媒体平台中收集到的 18 亿用户的个人信息。此次泄露的数据来源于架在亚马逊 S3 云存储上的数据库。由于配置错误导

致三台 S3 服务器“可公开下载”，其中一台服务器数据库中包含了近 18 亿条来自社交媒体和论坛的帖子。

2018 年 7 月 20 日，新加坡保健集团（新保集团）遭到网络攻击，约 1/4 的新加坡公民个人信息被非法获取，其中包括时任总理李显龙的个人信息及门诊配药记录，这起网络事件也被当地媒体称为“新加坡遭遇的最大规模信息安全攻击”。黑客先侵入新加坡新保集团的电脑，植入恶意软件后有目的地攻击信息系统数据库中的具体个人资料，反复尝试盗取和复制时任总理李显龙的个人医疗记录并顺利得逞。相关分析人士表示，一国在职领导人的医疗数据被黑客拿到，是此前闻所未闻之事。目前，大多数社交网站为强制实名制，因此使得此类用户的隐私信息更容易暴露在其他用户面前，如果黑客恶意利用此类信息那么后果将难以想象。可见，信息系统安全问题一旦暴露，将会对国家、企业或个人造成无法挽回的损失。近年来的重大信息安全事件，见图 1.1。

图 1.1　近年来的重大信息安全事件

网络信息系统的脆弱性影响系统的安全性。在网络系统中，脆弱性的分布和程度随网络结构组件的变化而变化，随着操作系统到各种应用软件的升级换代发生变化，攻击技术和方法也会发生变化。单纯的安全保护技术已不足以解决信息系统的安全问题，信息安全技术的先进性并不能保证国家、组织和个人信息系统的安全性。首先，信息系统安全技术自身存在可能被黑客利用的弱点或漏洞。例如，TCP/IP 协议集就存在着基本的安全缺点，如大多数低层协议为广播方式，网上的任何机器均有可能窃听到情报，较易推测出系统中所使用的序号，从而较容易从系统的后门进入系统等。由于每一层数据存在的方式和遵守的协议各不相同，而这些协议在开

始制定时就没有考虑通信路径的安全性，从而导致了安全漏洞的出现。其次，传统的安全威胁开始混合，网络袭击导致的大规模、长时间的网络故障和信息系统安全问题使人们遭受了越来越严重的损失。根据赛门铁克发布的2018信息系统安全威胁趋势，黑客会利用人工智能和机器学习等新兴技术，来对抗同样利用这两种技术进行安全保护的企业，这些攻击未来将会变得更加先进。再次，人们需要防范的已远不只是病毒而已，社会工程学已经被网络犯罪分子使用得得心应手，所以在使用第三方软件时也需要更加提高警惕。根据国家计算机病毒应急处理中心病毒样本库的统计，2016年我国计算机病毒感染率为57.88%，与2015年63.89%的感染率相比，下降6个百分点，其下降得益于广大计算机用户安全意识的提升、安全产品的普及和多级防护体系的建立。电子邮件是黑客利用社会工程学进行攻击的主要途径之一，黑客通常会发送一封看似正常的邮件，例如将发件人伪造成IT管理部门、收件人的领导或下属，来获取收件人信任，然后通过收件人下载或点击附件中的病毒、木马达到攻击目的。目前，社会工程学邮件攻击是网络钓鱼、勒索软件、APT攻击最主要的攻击途径。最后，黑客的攻击和企业的防守呈现不对称博弈的形势，包括工作量不对称、信息不对称和后果不对称。RSA执行主席Art Coviello引用了美国业内人士的话："安全是永远不可能成熟的一个技术领域，因为它的成熟并不取决于客户或者企业的要求，而是取决于那些犯罪分子的做法。"在暗处的黑客不知何时会突然发起攻击，就连Google这样的巨头都不能幸免。因此除了对已知威胁加强防范，对于未知威胁，企业需要进行实时监控和行为分析以进行检测。信息不对称表现为黑客可以通过网络扫描、探测、踩点对攻击目标进行全面了解，而企业对攻击方往往一无所知。黑客在攻击失败后极少受到损失，而企业安全策略被破坏后却利益受损严重。

综上所述，信息系统安全研究在技术、行为、管理、哲学、解决保护信息资产并减少威胁的组织方法等领域都有着深远的影响。将技术开发和管理理论相结合进行研究逐步成为信息系统安全领域中一个极为关键的任务，也是现代信息网络中重要的问题之一。科学地制定信息系统安全技术策略抵御复杂网络环境中的威胁以保护信息系统的安全性，已成为当前的重要任务。

1.1.2 信息系统安全技术研究趋势

随着信息系统安全事件的频繁发生，人们对信息系统的安全需求也逐渐增加（见图1.2），相应地，对信息系统安全技术管理策略的要求也发生了巨大的变化。目前，解决信息系统安全问题有两个非常显著的发展趋势：一是从传统的主要依靠安全技术向越来越强调将运用安全技术和加强安全管理紧密结合转变；二是从传统的主要运用单一技术向越来越强调组合运用多种安全技术转变。出现这样的研究趋势是有多方面原因的，主要包括以下几点。

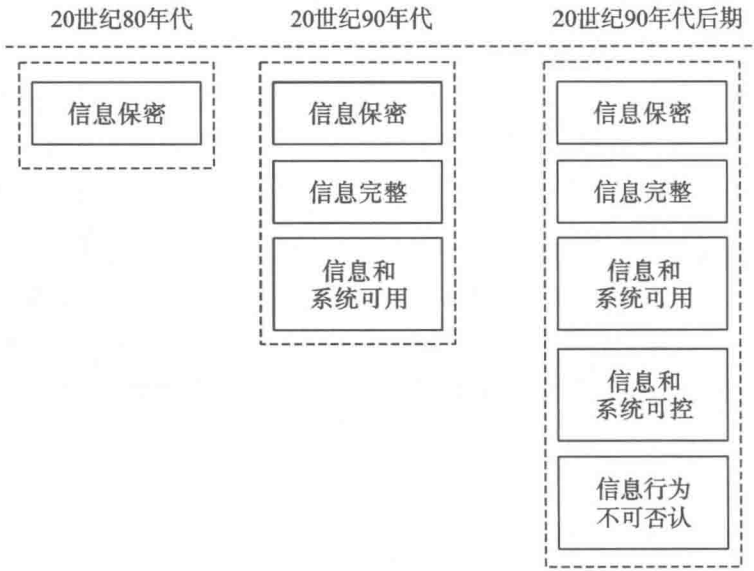

图1.2 信息系统安全需求的演变

第一，大量的调查发现，绝大多数信息系统安全问题是人为因素造成的，要有效解决信息系统安全问题，必须将技术、管理和法律法规等有效结合起来。当前一些企业对安全问题的认识还是停留在技术层面上，虽然投入了很多资金升级信息系统安全技术，却不知道信息系统安全状况如何、存在哪些问题。事实上，内部员工既可以是信息系统最可靠的安全防线，也可以是潜在的最大威胁。例如，一高管人员要求单独使用打印机，

并且要求与内部网和万维网相连，以便可随时用任何联网的电脑打印文件。于是，这台打印机有内存、中央处理器，并与网络相连，却在系统的防火墙之外，黑客便可通过这台打印机侵入内部系统。社会工程学也显现了信息系统安全中与人的行为相关的管理因素的重要性。早在20世纪90年代，著名黑客Kevin Mitnick使得“黑客社会工程学”这个术语流行起来。社会工程是指信息安全中操纵人的行为或泄露机密信息的手段，通过信息收集达到诈骗的目的或获得计算机系统的访问权限。例如，黑客可能诱骗用户相信来电者或来访者的虚假身份，获得企业职员认为无关紧要的信息（实际上它是有用的）。他们可能首先假冒服务中心，称出现网络问题，并套取到计算机端口号，然后冒充企业职员请求技术支持封掉端口号。被封掉端口号的企业职员请求帮助，黑客趁机介入，结果企业职员运行了黑客的木马程序。所以，凡是有可能接触到敏感、有价值或重要数据的人员，都必须时刻保持警惕性，在各自的领域发挥作用。可见，营造良好的组织文化、加强信息系统安全管理至关重要。信息系统安全不仅是技术层面需要关注的问题，而且是由于人的安全意识淡薄和管理不善而影响了整个信息系统的安全性。

第二，因为目前的网络环境下存在太多的潜在攻击者和众多的网络攻击手段，没有一种安全技术可以让信息系统完全应对来自系统内部和外部的各种攻击手段，组合运用多种安全技术保护信息系统可以增加攻击者实施攻击的成本。典型的攻击手段包含拒绝服务攻击、非法接入、IP欺骗、网络嗅探、中间人攻击、木马攻击以及信息垃圾等。随着攻击技术的发展，主要攻击手段由原来单一的攻击手段向多种攻击手段结合的综合性攻击发展，例如木马、网络嗅探、防拒绝服务等多种攻击手段的结合带来的危害将远远大于单一手法的攻击，且更难控制。为了保证信息网络的安全性，降低信息网络所面临的安全风险，单一的安全技术是不够的，应有相应的不同网络安全防护方法。例如，基于主动防御的边界安全控制、基于攻击检测的综合联动控制、基于源头控制的统一接入管理、基于安全融合的综合威胁管理和基于资产保护的闭环策略管理。攻击者的成本主要包括漏洞发现的成本、漏洞利用实现的成本、漏洞实施的成本、获取的信息资