网络防御经济学

网络威胁日渐猖獗的时代，
建立安全投资模型应对风险

JUNIPER NETWORKS

网络攻击防御经济学：网络威胁日渐猖獗的时代，建立安全投资模型应对风险

由瞻博网络（Juniper Networks）发起、兰德公司（RAND Corporation）开展的一项新研究“安全防御者的两难境地：制定计划维护网络安全”，推出了一个创举性的启发式模型，可帮助企业确定网络防御的经济动因和挑战。

网络攻击正在快速成为各界企业面临的最大风险之一。显而易见，不论是由于商业间谍活动而导致的知识产权损失，还是普遍得惊人的大规模数据泄漏，企业都必须要采取更多的措施，才能抢先于威胁一步，有效管理风险。对此，企业已经投入大量时间、精力和资源应对所面临的网络攻击带来的威胁。

企业在这方面的投入，有相当充分的理由。RAND公司去年开展了一项由Juniper Networks赞助的研究，名为“网络犯罪工具和被窃数据市场：黑客的集市”。该研究发现，网络攻击者已经建立网络黑市，其经济成熟程度前所未有。实际上，这些市场有助于攻击者更高效地渗透企业网络，并为其带来更多的利润。事实上，该研究预测，网络攻击能力将很快超越防御能力。

> Juniper公司坚信，尽管网络攻击者的经济运算一目了然，但对于企业来说，却依然面临更忙乱、更不明朗、更混乱的局面。

研究报告重要结果：

Juniper公司认为，RAND的新模型确定了影响企业网络安全成本的五大推动因素，详情请见本摘要内容和RAND公司的报告全文。每个推动因素现在或将来都可对成本产生显著的影响。

1. 完全通用的解决方案并不存在：企业没有采取最佳的投资策略
2. 许多安全工具都有半衰期，会慢慢丧失价值
3. 关注人力，势在必行：长期来看，人力方面的投资会降低成本
4. 物联网正处于十字路口
5. 排除软件漏洞，成本将大大降低

尽管安全行业多数人早已普遍认为这些推动因素是安全计划中的重要因素，然而RAND的研究首次量化了这些推动因素对成本的影响程度。这样做的目的是，这个新模型有助于为企业提供以数据为导向的见解，使企业理解每个推动因素的重要性及其如何帮企业更具战略性、更全面地管理安全风险。

安全防御者的两难境地

RAND公司的这项新研究剖析了防御方的经济现状，表明首席信息安全官（CISO）认为自己充其量只是在勉强维持现状，加大对安全的投资，却没感觉安全性比以往提高。更令人担心的是，他们认为网络黑客会很快赶上网络防御方，许多人都不确定他们在网络安全方面的投资是否足够，以及何时足够。

导致这一后果的部分原因是，许多公司甚至安全行业自身都缺乏足够的意识，没有将网络安全看做持续的企业风险。管理风险这个术语在网络安全中经常被错误理解；应注意的是网络安全威胁和漏洞带来的风险，而不是业务成果和运营带来的风险。人们注重的（甚至是用于体现安全计划价值的衡量标准）通常是某个特定工具或计划阻挡若干攻击的能力，而不是对于企业更为重要的衡量标准。

全面安全计划的目标，应该是了解风险控制投资的回报，或是投资风险减少了多少（RROI），而不是衡量阻挡了多少攻击。这就意味着要找到更好的方法来了解对网络安全风险影响最大的因素，以及怎样才能更有效地管理这些风险。

为了着手解决这方面的需求，Juniper Networks邀请并赞助RAND公司的经济学者和安全专家开展研究，探究影响组织网络安全风险成本的主要因素。该研究还调研了组织可以进行哪些投资，以便更有效地控制日益严重的网络攻击威胁对其声誉、信息和网络带来的风险。

RAND公司致力于提供的客观分析和见解，在帮助其他行业从容应对挑战方面已有卓著业绩，包括控制医疗花费、解决国家安全冲突和控制防御支出。让组织检查其业务方面的网络安全棘手问题，可帮助安全防护业界和从业者证实他们面临的许多挑战，并向企业高层提供关于如何解决这一问题的有力论据。

企业安全风险的启发式模型

RAND公司的举措关键在于开发出一个前所未有的启发式模型，该模型可为企业提供一个学习工具，帮助企业更加了解影响安全风险管理成本的主要因素，以及影响成本的各种投资决策。通过观察这些因素会如何交互，模型提供了一个框架，可供用于思考不同的网络安全决策所带来的不同影响。

尽管目前已经存在数种很有价值的安全风险模型，如操作性关键威胁（Operationally Critical Threat）、资产和弱点评估（OCTAVE）以及信息风险因素分析（FAIR），这些模型都可以帮助企业了解其面临的具体风险和识别最需要保护的信息，但RAND模型是第一个确定网络安全风险管理整体成本的模型。该模型通过考察企业做出不同选择的方式，引入新型科技，调查黑客行为，这些因素相互作用并影响着网络安全的成本。

为了对风险进行全局把握，RAND公司的模型研究了组织寻求网络安全成本最小化的方法。网络安全成本包括预防网络攻击所产生的直接和间接成本，以及遭受攻击产生的潜在损失，按存在风险的信息的价值和遭受攻击的概率进行衡量。

> RAND公司的模型是首个能测量管理网络安全风险所产生的整体成本的框架

RAND的模型包含27个影响组织10年期间成本的参数，以确定组织需承担的成本。对任一参数进行调整，即可查看该参数对成本的影响。

这些参数总共可分为三类：

1. **组织特征**：组织的规模、使用网络的电脑/设备数量和存在风险的信息的价值。
2. **安全计划与投资**：模型可供企业就四种工具的使用做出决策，使用每一种工具都有成本，也会降低遭受攻击的概率：
   - 购买和使用安全工具的直接成本
   - 开展员工网络威胁进阶培训的直接和间接成本
   - 对智能设备和空气间隙（尤其是敏感的子网）采取限制造成潜在生产力损失而造成的间接成本
   - 安全防护人员执行安全计划的尽职程度
3. **生态系统的变化**：技术生态系统的变化如何影响安全防护成本。例如，采用更多物联网（IoT）设备如何改变攻击范围，或是某一年推出的软件安全漏洞如何影响黑客袭击的可能性以及随之产生的成本。

实际上，Juniper公司认为，该模型为首席信息安全官（CISO）提供了一个系统性起点，能帮助他们理解自己可以做出不同的决策来保护所在组织，并得到高管层更多支持。

> 模型为首席信息安全官（CISO）提供了一个系统性起点，能帮助他们理解自己可以做出不同的决策来保护所在组织，并得到高管层更多支持。

为此，Juniper开发出对该模型的交互式解译，帮助企业在组织中应用诸多参数。这可帮助用户通过改变对成本影响最大的主要变量，开始判断企业应该如何进行安全防护投资。

最终，该模型的设计会兼具指导性和诊断性，因为每家企业都会有各自的独特需求和挑战。不过对于想要在组织内得到更多支持的安全专家来说，这是一个强有力的起点，也是一个谈判的工具。

如有企业和决策者想全面了解*RAND*公司的模型，可参阅报告全文的附录，了解模型所采用的方法论。

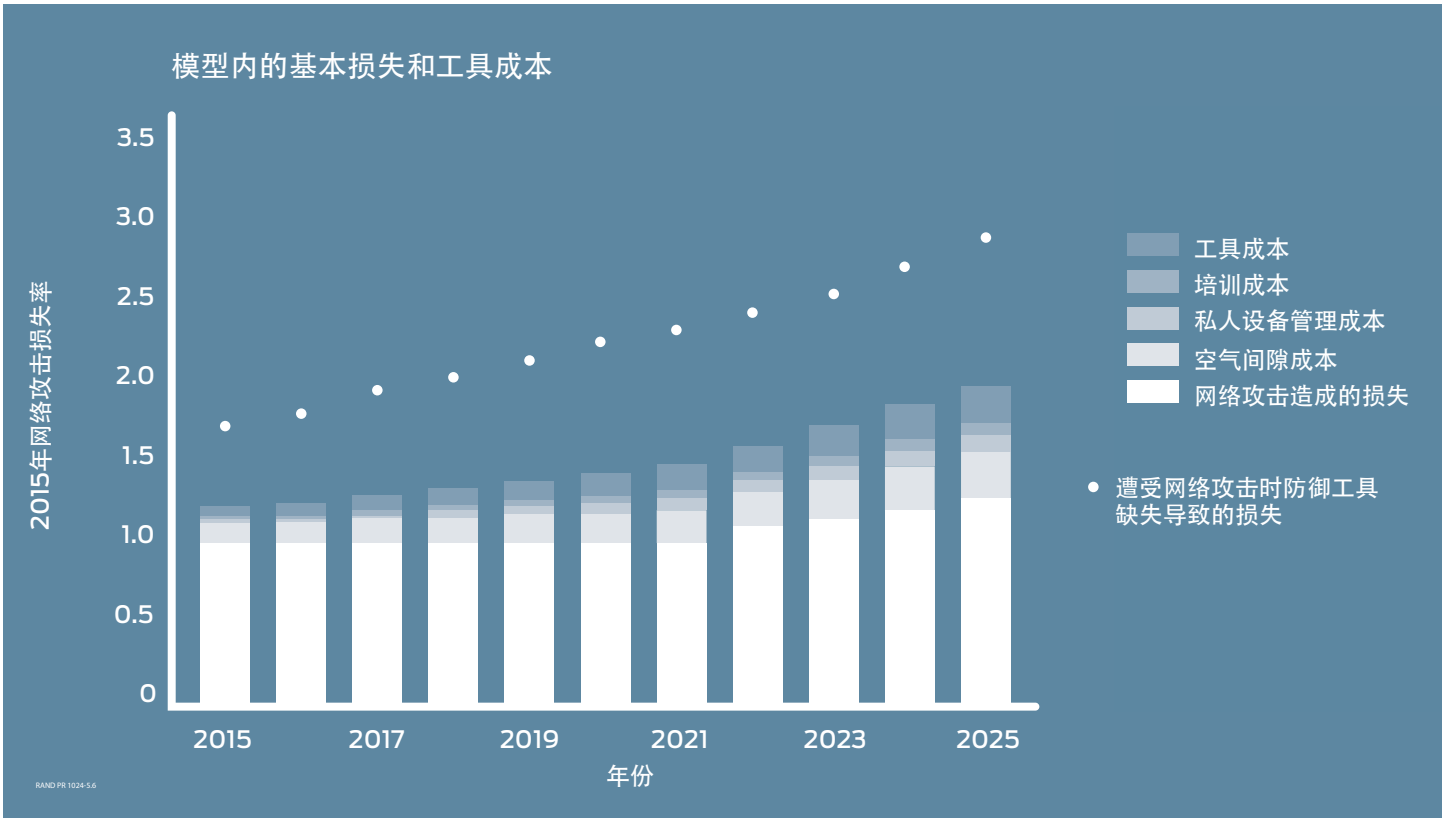
模型传达的安全进程相关情况

比模型如何运作更加重要的是它所生成的见解。RAND公司的报告详细介绍了一个使用该模型的基本案例，案例从整个企业界的视角衡量成本，以及在模型运作的10年内成本如何变化。

RAND公司的模型表明，所有行业管理网络安全风险所产生的成本将在未来十年增加38%。

> 预计在未来十年内，所有行业的网络安全风险管理成本将增加38%。

有趣的是，对需要控制潜在损失的公司来讲，大部分的成本之所以增加不是因为网络攻击本身所导致的损失增加，而是来自安全计划成本的增加（例如，在工具和培训方面的投资、限制携带个人设备/智能设备以及网络空气间隙）。然而，这些投资最终会产生成本效益，因为如果不进行投资，损失将会更大也会增长得更快。在下表中，虚线表示的就是在不投资网络保护的情况下，公司所遭受的损失情况。



首席信息安全官的主要成本因素

RAND的模型也为企业提供了很有价值的见解。Juniper认为，企业在进行安全防护措施时，必须要考虑到RAND模型中提到的五大成本因素。尽管这些因素对于安全防护业界的多数人来说只是普遍接受的经验之谈，但RAND的模型确认了这些因素的重要性。

1.完全通用的解决方案并不存在：企业没有采取最佳的投资策略

RAND的研究表明，许多公司在投资方面可能不会采用最佳经济策略。安全工具的最佳数量、人员培训、个人设备限制和决定需要切断哪些网络与互联网的连接，这些均因公司而异。

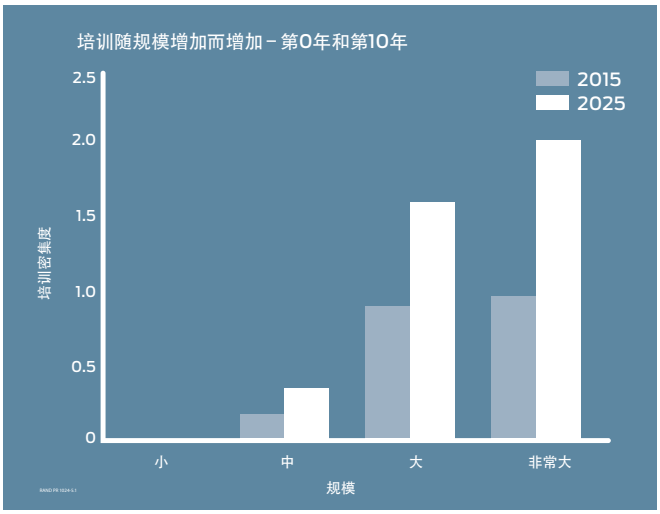
中小型企业

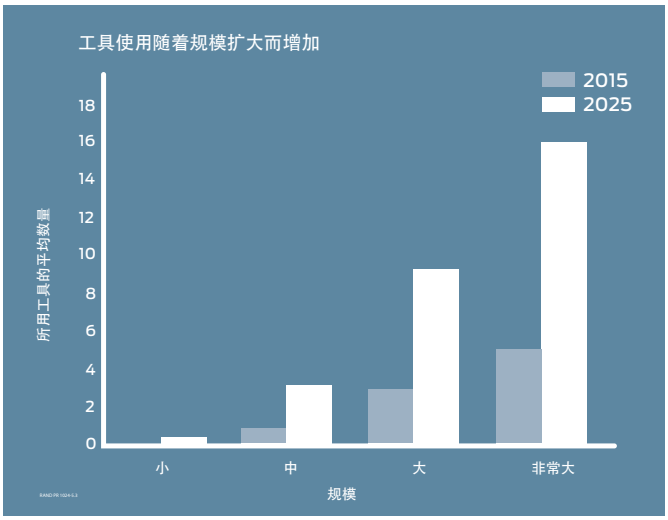
中小型企业（SMB）可从基本工具和政策方面受益，但不会在综合安全培训和安全防护高科技方面过度投资。因为中小型企业的受攻击范围要小得多，遭遇高级黑客攻击的可能性也较小，相对于他们出现安全漏洞的可能性因此遭受的潜在损失，在高成本安全防护上过度投资会不成比例地增加成本。然而，基本工具和政策能最大化保护中小企业，帮助他们维护网络安全，并限制网络中个人设备的使用。

大型组织和高价值企业

另一方面，大型组织和/或拥有高度敏感信息的组织，如防务承包商或有大量知识产权的组织，都需要投资全方位的政策和工具。他们受到高级黑客攻击、遭受频繁的日常攻击，或者面临某类型入侵的可能性要大得多。如果企业不在这方面大力投资，那么一次事件就可导致巨大的损失。

另外，大型组织在安全投资方面也会有更大量级的收益。例如，随着员工数量的增加，为每个员工提供进阶安全培训的成本效益也会提高。





假设进行基本的安全意识培训，并有出色的工具可使用。

2.许多安全工具都有半衰期，会慢慢丧失价值

公司所面临的最大挑战之一是针对黑客用于避开公司防护措施的反制手段。黑客一直致力于开发反制手段对付新的安全技术，这就限制了这些工具随着时间推移的相对有效性，也要求企业投资采用新的技术来取代旧的工具。

我们以探测系统，如沙箱或杀毒程序为例。尽管这种防护工具在刚发布的时候非常有价值，也是大型组织的安全防护中必不可少的一部分，但这种手段很容易受到反制手段的影响。所以，要让这些工具有效地防御黑客攻击，必须对它们进行不断的重新评估，并找到新的解决方案。措施催生出反制手段（敌对动态）差不多可以概括导致网络结构形成的根源。

这种结构最终会迫使企业必须在安全技术上加大投入，才能将保护能力维持在原来的水平上。这同样增加了公司的运营成本，因为公司需要引进的安全技术种类与日俱增，也需要公司的安全团队进行管控。

RAND公司的模型预测，随着时间的推移，面对反制手段，这些技术的有效性在十年内会降低65%。因此，从该模型运行的第一年到最后一年，所有企业在安全工具方面的支出占该公司总安全防御支出的比例会上升16.2%。如果排除背景信息，这个数字对某些企业看似微不足道，但考虑到安全工具是企业安全防御中最大的一笔支出，这个增量将又是一笔巨款。

那么企业应该将投资重点放在哪里？RAND公司也发现，某些类型的安全工具不易收到反制手段的威胁。用于提高安全和补丁管理、自动化、改善政策在公司内部执行情况的技术和安全功能都属于这一类，因为黑客不会试图避开这类工具。

大部分企业最终都需要搭配使用各种类型的工具，来保护自身的系统。然而，Juniper认为最重要的是，企业必须了解并在评估新一轮投资时谨记这种动态机制的存在。

易受反制手段影响的

- 反常检测
- 特征检测
- 沙箱恶意软件
- 反攻
- 反钓鱼培训

不易受反制手段影响的

- 防火墙政策执行和自动化
- 多因子鉴别
- 自动化补丁管理和补丁版本监测
- 子网隔离
- 入网控制

3.关注人力，势在必行：
长期来看，人力方面的投资会降低成本

RAND模型提出的其中一个因素从长期看可以大幅降低安全成本，就是培训投资以及建立尽职的安全防护团队。一支由博学的精英成员组成的安全团队能抵得上甚至更优于投资新的安全工具。如果管理不当，就算最好的工具也起不到应有的效果，这一点也在模型的考量范围内。

根据RAND模型，比起拥有懒散的安全团队的公司来说，如果一个公司的安全团队兢兢业业，能够高效地管理安全计划，则该公司第一年的网络安全成本将降低*19%*，到了第十年，则会降低*28%*。

Juniper认为，尽管网络安全方面极缺博学的专业人才，但这些潜在的费用节省空间价值极大，不容忽略。企业必须极力培训并迅速扩张自己的安全团队。如果无法招到新员工，另一个可用的方法就是将专业的安全任务外包给其他专家。RAND的报告显示，充分利用这类托管服务可带来以下好处：

> 许多防御者选择将某些重要的防御任务，外包给可为各种客户提供特定的服务专家团队。例如，许多大型组织没有进行网络渗透测试，因为这方面的培训太专业化，很难雇到相应的专家，也很难将本公司员工的能力维持在最高水平。[1]

2015

尽职程度	攻击成本的差异
非常低	增加 13%
低	增加 10%
中	中等
高	中等
非常高	降低 6%

2025

尽职程度	攻击成本的差异
非常低	增加 18%
低	增加 13%
中	中等
高	降低 6%
非常高	降低 10%

[1] “安全防御者的两难境地：制定计划维护网络安全”RAND公司，2015年，作者Martin Libicki、Lillian Ablon和Timothy Webb。

4.物联网正处于十字路口

关于物联网的话题非常多，其中不乏一些过度宣传。但有一件事是确定的：在不久的将来，企业将会有比以往更多的设备连接到网络中。根据RAND公司的报告，物联网将会对整体安全成本产生影响；不过，无法明确会是积极的影响还是消极的影响。Juniper认为，这会将企业推向一个十字路口。

如果企业能够通过灵活、成熟的方式应用安全技术和设备管理，正确处理物联网带来的安全影响，那么随着网络中的设备数量超过传统个人电脑的数量，他们就能看到长期的回报。另一方面，如果物联网也踏上早期个人电脑走过的路，从而引发各种安全问题，企业将会面临安全成本飙升的局面。

RAND的模型显示，在后一种情况下，由于网络黑客袭击在过去10年中上升了*30*%，物联网的引入将增加企业的损失。

尽管大多数企业距离感受到物联网的真正影响还有数年之久，但Juniper公司认为，这些企业应该早做打算，从现在开始就考虑如何将这些设备纳入公司的安全计划和网络当中。企业将需要确保其安全基础设施足以管理这些新设备和接入所带来的带宽。

此外，企业将需要决定采取哪些安全管理措施，以对企业环境中的新设备进行监管。与私人设备的管理相似，企业必须要确保他们有合适的工具，在不远的将来物联网接入其网络的时候，快速提供并管理这些连接。这包括建立和执行正当权益管理，确保这些新设备不会扩大受攻击范围，以及对员工在工作场所使用个人物联网设备制定明确的公司政策。

5.排除软件漏洞，成本将大大降低

RAND公司认为会对成本产生巨大影响的一个方面是软件漏洞和员工所使用应用程序的数量。企业经常会发现由于基本系统和软件不安全，他们不得不对防御措施进行投资。遗憾的是，这一指标很大范围内是首席信息安全官无法控制的，它取决于软件制造商设置更多安全码。

*RAND*的模型发现，如果软件漏洞的发生率降低一半，企业网络安全方面的整体支出将降低*25*%。

但是，软件漏洞在未来是否会减少，这一点无法确定。如果网络和软件架构是静态的，防御者就能够在最终占得上风，但创新是信息科技的生命力所在。

RAND的研究表明，新的漏洞数量可能会随着物联网设备的剧增和软件生态系统在前一版本安全码的基础上日益复杂而增加。

好消息是，业界做了许多工作来提高软件的质量。例如，开发者可以用免费的工具来帮助他们在发货之前识别漏洞。随着越来越多的软件制造商使用这些工具，产品中发现的漏洞可能会越来越少。

Juniper认为，企业有责任仔细检查他们所使用的软件，要求软件提供商采用进行更好的安全测试和补丁。如果因安全因素导致公司停止某个程序，那么软件制造商将会有更强烈的动机，开发出更优质、漏洞更少的产品。

企业和行业的前路

那么在网络威胁日益猖獗的今天，企业可以采取哪些措施更好管理他们的安全风险投资呢？

象管理企业一样管理安全措施

企业应该找到更好的方法，像管理企业一样管理安全性，即量化不同决策带来的风险和好处。Juniper公司认为，RAND模型提出了多个企业在评估安全状态和支出的时候应该考虑的可执行见解。

而最终，首席信息安全官应尽力制定更好的衡量标准来确定PROI。总而言之，企业必须像为公司管理股票组合一样，不断评估计划的生命周期和有效性。这就是Juniper公司对该模型的交互性解译，RAND的模型和方法论有助于公司在考虑自身需求的情况下，判断哪些工具在解决这些需求时最为有效。

评估安全工具时谨记反制手段

根据RAND公司的发现，“组织决策可能会/应当会受到反制手段的影响，不论进行什么样的投资，尤其是在系统防御方面……企业应该考虑采用更不可能引发反制手段的策略。”

Juniper认为，这意味着企业应优先对通过集中管理和分散执行平台进行安全任务自动化的工作进行投资，尤其是在防护网络安全方面。自动化是Juniper公司的主要关注领域，我们鼓励客户考虑投资自动化工具，出于以下几个原因：

- 内置自动化的工具较不容易受到反制手段的影响，这也使得他们能保持长期的有效性和价值。
- 通过降低对已经压力重重的IT团队的运营要求，自动化能够减少组织的其他安全成本。
- 自动化能让安全防护人员减少花在配置和测试系统的时间，让他们将更多精力放在其他重要任务上，如解决面临的最复杂攻击，以及加强防护系统。
- 最后一点，集中系统有助于让安全投资易于管理和执行，以此增加其他安全投资的益处。例如，对威胁检测信息来源实行自动化的集中管理，有助于对不同威胁信息来源混杂为一体的情况进行快速处理，并找到网络中的强制点。

如需了解更多关于Juniper在自动化方面的工作和投资，请访问这里。

呼吁业界采用行动

推动安全防护的系统性进展不能由首席信息安全官一肩承担。Juniper认为，整个安全防卫行业和政府务必采取重要措施，改变目前的动态机制，在防御工作上起决定性作用。

培训下一代

抢先于黑客一步的一个关键是培训下一代开发者，让他们更好地保护自己的创新。RAND的报告同样也支持这一观点，报告称“……安全编码并不是电脑科学专业标准课程中的一部分。这些学生是开发和创造这些设备的下一代人才。”

如果通过培训能让下一代创造出本身更加安全的软件，企业数据泄漏的可能性会大幅降低，从而也会减少企业在安全方面的总体开支。

培训下一代学生在安全防护方面的能力，这也意味着下一代有更多的人会成为安全防护专家，并在岗位上更高效地完成工作。通过现在开始建立人才梯队，安全防护行业终将能够解决当前专业人员缺乏的问题。此外，通过学习黑客道德规范，许多可能受到蛊惑进入黑市的未来黑客更有可能把他们学到的技术用在好的方面。

开发技术时谨记反制手段

此外，安全创新者（如Juniper）必须继续研发安全技术，用以抵御攻击者的反制手段，提高网络透明度并有效控制网络。尽管攻击者和防御者之间的猫捉老鼠游戏将继续并一直存在，加大力度来应对这种现象可以增加攻击者研发出新技术的难度。

我们并不断言本报告或模型能够提供了解网络安全风险的最终方案。安全防护行业应从这里开始，探讨它如何见解风险。我们希望我们与RAND所做的工作能够推动讨论再进一步。

RAND公司的报告全文，以及Juniper去年的报告及补充材料都可以在这里查阅。

关于本报告

“安全防御者的两难境地：制定计划维护网络安全” 由RAND公司的安全专家Martin Libicki、Lillian Ablon和Timothy Webb共同编制。本报告基于2013年10月至2014年8月与多位首席信息安全官就当前和未来的威胁现状进行的深度访谈。在Juniper赞助下，RAND公司编制了一个分为两部分的系列报告，本研究是在第一份报告“网络犯罪工具和被窃数据市场”的基础上开展，调研了网络攻击者背后的经济推动因素，以及他们所建立的成熟的地下黑市。

公司和销售总部

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
电话：888.JUNIPER (888.586.4737) 或
+1.408.745.2000
传真：+1.408.745.2100
www.juniper.net

亚太（APAC）和欧洲、中东和非洲（EMEA）总部

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
电话：+31.0.207.125.700
传真：+31.0.207.125.701

版权所有 2015年 Juniper Networks, Inc.保留所有权利。Juniper Networks和Juniper Networks的标志都是Juniper Networks, Inc.在美国和其他国家的注册商标。其他所有商标、服务标志、注册商标或注册服务商标均是各自商标拥有者的财产。对于本文中任何不准确之处，Juniper Networks均不承担任何责任。Juniper Networks保留更改、修改、转移或以其他方式修订本出版物的权利，恕不另行通知。

Juniper Networks (NYSE: JNPR)致力于实现路由、交换和安全领域的创新。Juniper Networks在软件、硅和系统方面的创新改造网络经济的历程。如需了解更多信息，请访问Juniper Networks官网（www.juniper.net）或在Twitter和Facebook上关注Juniper。