预测未知威胁

首席信息安全官 (CISO) 基准研究报告

CISCO

目录

简介：深入洞察，高效阻止

试想一下，如果您既能够洞察未来，又能够回到过去；既可以看到任何地方曾经发生过的一切事情，同时又可以看到将要发生的一切事情，那会怎样？

再试想一下，如果能够具备强大的处理能力，准确理解各种语言、各种维度的各种数据，那会怎样？除非您已经达到了这种全数字化数据的理想境界 （并且还没有告诉其他人），否则世界上总会有一些您不知道的事情。

在安全领域，企业外部的未知威胁形式多样，包括恶意攻击者、国家资助的攻击和恶意软件，这些威胁传播迅速，所到之处疮痍满目。企业内部的未知威胁形式包括员工的恶意行为或承包商的粗心之举造成的内部威胁。24% 的调查受访者认为，内部未知威胁给他们的组织带来的风险最严重。未知威胁包括新设备、新云应用和新数据带来的威胁。未知威胁让 CISO 们彻夜难眠，我们知道这一点，因为我们进行过调查。

这是我们连续第 12 年发布关于网络安全形势的研究结果，也是我们第五年对数千名安全领导者进行基准研究。调查获得的数据非常多，而这份报告只是冰山一角。在未来一年里，我们将按行业、地域、公司规模和工作职能以及其他筛选条件来发布更多基准数据。为了发布这份报告，我们对 18 个国家/地区的 3200 多名安全领导者开展了调查，向他们询问了以下三方面的问题：

1. **准备**：您如何通过培训、预算、演练、最佳实践和其他核心竞争力措施为自己的成功做好准备？
2. **架构**：您采取什么方法来选择供应商/解决方案和管理警报？
3. **攻击应对准备和及时应对**：您如何根据受影响的系统、损失程度以及恢复时间来管理攻击事件？

采访 Marisa Chancellor，思科安全和信任组织高级总监

思科拥有七万名员工，他们遍布 400 个办事处，共使用数十万个终端设备，您能为这么多人提供防御保护，实在令人钦佩。

所以可以说，我们的受攻击面很大，为了实现这种大规模的防御，我们可以尝试做很多事情。我们不仅有员工和数据中心，还使用 600 个云，因此我们要保护的其实是一个多云和混合云环境。

请介绍下您的团队宗旨。

我们受命为思科提供防御保护，努力平衡思科作为企业所面临的运营风险与内外部威胁所带来的风险。我们的工作重点是，通过分析所发生的事件确定我们的安全态势稳定性，将正确的安全架构引入我们的 IT 组织。

（续）

然后，我们比较了这些方面的绩效，看看自从我们开始跟踪以来，您是否在构建防御、检测网络威胁以及控制数据泄露方面取得了重大进展。此报告阐明了哪些措施在加强组织网络安全方面卓有成效，以便您可以向同行借鉴成功经验。

例如，调查过程中，只有 35% 的受访者表示“可以轻松确定攻击影响范围，进行遏制，并对漏洞攻击采取补救措施”，这表明洞悉未知威胁显然是一项主要挑战。也许正是“轻松”才导致您措手不及，因为事件往往不是表面的样子。不过，这意味着调查中有 65% 的 CISO 有改进的空间。然而，有 46% 的受访者表示“有相应的工具帮助执行审查，并提供有关安全实践能力的反馈”，这让我们感到了少许安慰。如果您承认无法具备彻底全面的洞察力，至少您可以衡量和管理这种洞察力，并努力提高。

虽然防御之战远未结束，但我们也并非一事无成。在我们的调查中，至少有一些受访者似乎对自己的工作很满意。我们询问受访者是否出现了网络防御疲劳，也就是几乎已经放弃尝试提前防御恶意威胁和恶意攻击者。只有 30% 的受访者表示今年出现了网络防御疲劳。虽然近三分之一的受访者认输了，这个数字看起来很多，但相比去年的 46% 已有所下降，这说明情况正朝着正确的方向发展，值得一搏。

（续）

什么问题会让您彻夜难眠？

我认为对于大多数从事安全工作的人来说，让我们夜不能寐的是未知威胁。尽管我们拥有优秀的团队和非常出色的技术，但一想到自己每天必须保护很多东西，而我们关注的只是已知威胁，真正的危险却来自未知威胁，我就寝食难安。

很多 CISO 向我们表示他们的警报数量非常多；您是否认为警报数量太多，难以管理？

整个行业都是如此；但在思科，我们每天都会查看 47 TB 的网络事件数据，大概平均每天 22 个事件，光靠人工是无法弄清楚的。这些数据来源广泛，我们必须弄清楚如何分析所有这些信息，以及如何让技术为我们服务。我们能够利用机器学习和人工智能来剔除大量警报，以便深入了解最应关注的风险领域。我们的预算有限；在这种情况下，我们如何以计算机的速度而不是人工速度来开展工作？

请参阅本报告中有关 Marisa Chancellor 的更多访谈摘录。

如果您认为同时洞悉未来和回到过去的能力似乎难以实现，我们就来改进当前的洞察力，比较现在和以往的报告数据，了解一下哪些方面有所进步，哪些方面不尽人意。

“我们的安全和信任组织负责保护思科；就这么简单。
但另一方面是，我们如何确保能够加快业务发展？
闭关自守对我们没有任何好处。”

Marisa Chancellor
思科安全和信任组织高级总监

回顾过去，展望未来

在过去一年里，CISO 工作是否有改进？我们挑选了去年比较热门的三个主题，并根据今年受访者的回答进行了评估。

	调查结果 2018 年	调查结果 2019 年	我们想要进行更深入了解，因为...
技术			
机器学习 (ML) 您在多大程度上依靠 ML 来减少保护组织安全所需的工作量？	77%	↓67%	对于技术领域的这三个方面，受访者的依赖性下降，可能是由于不确定性和缺乏信心。或者是机器学习还没有准备好大展拳脚。无论是哪种情况，我们都希望了解更多信息。
人工智能 (AI) 您在多大程度上依靠 AI 来减少保护组织安全所需的工作量？	74%	↓66%	可能是因为人工智能已经广泛采用并集成到您的业务流程中，以至于您觉得没必要将其分离出来进行计算。
自动化 您在多大程度上依靠自动化来减少保护组织安全所需的工作量？	83%	↓75%	您可能选择不“依靠”自动化，而是选择性地部署自动化。即使是大型组织也可能无法完全接受自动化。
网络攻击造成的损失			
过去一年里，您遇到的影响最大的攻击总共造成了多少损失？	8% 的受访者表示 500 万美元以上	8% 的受访者表示 500 万美元以上	网络攻击还会消耗大量资源，其影响不仅限于财务方面。
	低于 50 万美元 47%	低于 50 万美元 ↑51%	50% 以上的受访者将网络攻击损失控制到了 50 万美元以下；非常好。损失略有下降，或者至少得到了控制。
为更好地保护公司免受安全攻击影响，您作出了哪些改进？			
分离 IT 职能和安全职能	38%	↓35%	这是一个有争议的话题，两年的数据无大幅波动，表明组织平均分配了这两种职能。
提高员工的安全意识并加强培训	38%	↑39%	只要人员依旧是最薄弱的环节，就仍然无法确定需要多少培训才足够。
实施风险缓解技术	37%	↑39%	今年，20% 的受访者表示对风险和合规性不太了解，因此采用风险框架应成为标准操作程序。
增加对安全防御技术或解决方案的投资	41%	↑44%	如果能与培训和基于成果的衡量措施相结合，则效果会很好。很好的安全指标。
云			
将安全防御迁移到云端提高了我们的效率，使我们的安全人员能够专注于其他方面的工作	92% 赞同	↑93%	组织出于合理原因继续采用云。
利用云安全解决方案比采用内部部署方案更有效	91% 赞同	↑93%	对云安全的信心略有提升？我们会采用它！
保护云基础设施免受网络攻击的挑战性有多大	55% 非常困难	↓52%	保护云基础设施的难度大幅下降？非常好！

来源：思科 2019 年 CISO 基准研究报告

CISO 现状

一段时间以来，威胁搜索人员一直在谈论如何了解未知的威胁。现在是时候将其扩展到整个网络安全领域：用户、应用、数据和云。如果看不到威胁，就无法进行防御。

您通常想要为企业提供支持，不让企业因为官僚体制而陷入困境。如果要更加开放一点，应该如何减轻控制？每个人的答案可能不尽相同。CISO 必须处理组织文化的这种平衡，同时应对最严重的威胁。有时进行全面阻止和封锁并不符合企业的文化。这种措施可能适合银行，但却不适合大学之类的组织机构。

无论组织规模大小，CISO 在管理网络风险方面都面临若干挑战：

- 网络攻击会对组织的盈利能力、品牌声誉、客户数据安全、客户满意度和业务连续性造成不利影响。
- 阻止可能遭受巨大且无法挽回的损失，使组织的可保性面临更高的风险评分。
- 多年来，供应商单点解决方案看起来前景不错；但每个解决方案都会分别生成一系列警报。许多单点解决方案力求在警报方面做到无一遗漏以提高竞争力，这导致阻止难以识别那些给组织带来最高风险的威胁，因而造成资源浪费。
- IT 通常在整个组织中孤立存在，使得采取集成方案保护网络、云和员工终端变得非常复杂。

“我们需要努力了解如何洞悉未知威胁，例如即将发生的新型威胁，甚至是自己环境内部的威胁：未知设备、应用、数据。如果看不到威胁，就无法进行防御。这是让我夜不能寐的首要原因。”

- 需要采用积极的策略来聘用安全 IT 人员，因为专业人才资源短缺，无法应对全球组织面临的严重问题。然而，人才短缺问题难以控制，无法通过尝试填补所有工作岗位来解决。
- 新型威胁每天，甚至每小时都会出现，而且会采用更隐蔽、更复杂的方法。最近在 2019 年思科威胁报告中，我们报告了 Emotet、Olympic Destroyer 和其他比较活跃的威胁。威胁响应必须不断发展，需要使用工具来整合信息并对感染和其他事件进行集中补救。

CISO 要考虑的其他技术和流程包括：

- 使用正确的 AI 和 ML 技术对于将分流工作量至关重要。
- 网络攻击造成的损失在下降，但不要过于乐观。
- 有足够的空间来实现培训等流程改进的明显优势。
- 人们对云提供的安全性和保护云的信心增强。

2019 年结果

基准研究报告结果揭示了对加强组织安全状况至关重要的若干方面。本部分详细介绍了我们的研究结果，描述了在最佳实践、架构方法和网络攻击应对准备主题下，CISO 及其同行在哪些方面如何部署技术和流程，以减轻网络攻击对组织造成的影响。

准备好迈向成功了吗？

成为一名日常运营 CISO 意味着什么？您的宗旨是什么？我们目前的调查显示，有多个方面共同决定了组织的网络运行状况，包括：以务实的态度面对风险、制定预算标准、跨部门协作、提供员工培训、进行演练、了解如何跟踪成果以合理调整投资，以及对供应商和解决方案实施采取战略措施。

了解您的风险

进行风险管理就能有安全保障吗？几乎没有。需要了解网络攻击的风险以及包含安全漏洞管理的合规性环境，这对于理解如何防范和应对最坏情况至关重要。当被问及谁对风险和合规性非常了解时，只有 80% 的受访者表示自己非常了解。这样便有 20% 的安全专业人员可能要利用我们之前讨论过的一些培训。未知威胁越来越多，让您防不胜防。

如何利用预算

近一半 (47%) 的受访者在决定如何根据组织安全结果目标控制安全支出。衡量投资成果是最好的数据驱动方法。而且，98% 的受访者强烈赞同或基本赞同，他们的高管团队已建立明确指标来评估他们的安全计划的成效。49% 的受访者表示拥有供公司多个领域使用的指标，用于了解基于风险的决策并改进流程，以衡量整个组织的安全效力。

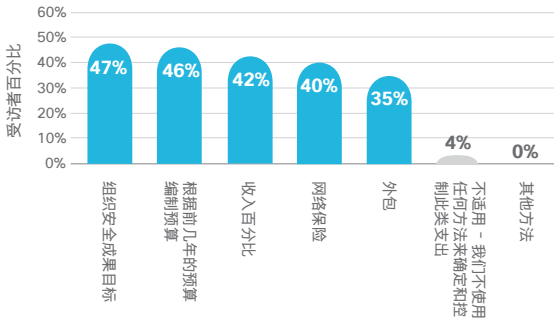
回到预算方面，除了基于成果的衡量措施外，如图 1 所示，还有一些在提升安全性方面稍逊一筹的选择：根据前几年的预算来控制安全开支 (46%) 和按收入百分比 (42%) 来控制安全开支都是常见的做法，但不一定能有效提升安全性。

“在某些领域，风险并不高，因为组织拥有强大的安全实践；在其他领域，我们有机会提供支持，最大限度减少并消除这种风险鸿沟。这样我们既能保护投资，又能准备好应对未来威胁。我们必须思考，我们可以如何建立基础架构，以便为随时可能发生的风险做好最充分的准备。”

网络攻击形势逐年变化，上一年的预算或收入百分比可能与未来威胁造成的损失几乎没有关系。

确定安全支出的第四个常用方法是网络保险：**40% 的受访者使用（至少部分使用）网络保险来制定预算。**采用这种方法首先要进行风险评估，以准确识别安全风险，并确保这些风险可以通过保险减轻或通过控制措施防护。对于某些公司而言，网络保险准则可能会在技术选择和/或预算制定中发挥作用。无论哪种方式，都值得在后续报告中进行进一步调查。

图 1 您的组织使用以下哪项来确定和/或控制安全支出？
受访者百分比，N = 3,259

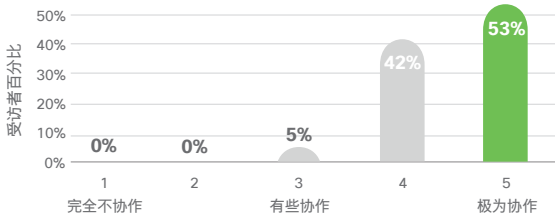


来源：思科 2019 年 CISO 基准研究报告

以协作取代孤立

在以往的调查中，受访者表示他们将安全职能从 IT 部门中分离出来，并且设立了 CISO 职务。幸运的是，你们与网络同事实现了良好协作。图 2 显示 95% 的受访者认为网络团队和安全团队之间协作程度非常高或极其高。你们不是在孤军奋战，这具有切实的财务优势。

图 2 不同职位的受访者报告的整个企业中网络团队和安全团队之间的协作程度。
受访者百分比，N = 3,248



来源：思科 2019 年 CISO 基准研究报告

协作带来了多少财务效益？事实证明，**在表示网络团队和安全团队之间非常协作/极为协作的受访者中，59% 的受访者遭遇的影响最大的网络攻击财务损失在 10 万美元以下，这在网络攻击造成的此类损失中是最少的。**

这显然值得进一步分析，可能表明对 DevSecOps 团队的需求有所增长，而且这种团队可能会进一步发展。协作不是碰巧的事，而是必须要做的事，特别是在敏捷开发时代。

最高管理层对此表示认同。根据 IDG 最近发布的 CIO 研究报告，“82% 的 CIO 希望他们的 IT 和安全战略能够在未来 3 年内紧密融合。”*

* 来源：安全联盟：CIO-CISO 的关系如何加强 IT 和业务，IDG，2019 年 2 月

“人们之所以落入网络钓鱼的陷阱，很大一部分原因在于情绪反应，黑客就是在利用这种情绪反应；他们试图引发情绪反应，所以我们在与员工进行网络钓鱼模拟时就会尝试这么做。所有模拟都是基于情景的，设想有一封邮件告诉您有一个包裹在等待您处理，谁不想赶紧发送或签收呢？”

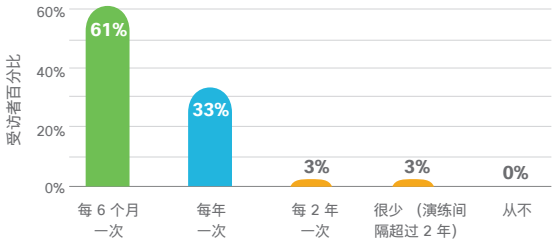
员工参与：演练

有人会问，“如果我们为员工提供了培训，而最后员工却离职了，该怎么办？”。“如果我们不提供培训，而员工却没变，又该怎么办？”在安全方面，也存在同样的问题。诚然，我们关注技术，但我们也应该在流程和人员方面花费相同的时间，因为员工是帮助保护组织安全的一线人员。

如果人员/用户被认为是安全领域最薄弱的环节，通常就应该制定相应流程，从新员工入职时就开始着手改善。您也可以考虑一下这个事实：只有 51% 的受访者表示，自己在通过全面的员工入职管理以及处理员工调动和离职的适当流程，从而管理安全人力资源方面表现出色。只有 39% 的受访者表示在事件发生后随即对员工进行培训，该趋势与去年同比持平，这似乎也不合理。

如果没有进行适当的防御准备，灾难的影响可能非常惊人。这个方面可能有改进的空间，因为 61% 的组织每六个月进行一次演练，以测试对网络安全事件的响应计划（图 3）。演练可以增强执行适当控制的能力，以便尽快做出检测和响应，从而减轻损失。

图 3 组织多长时间演练一次网络安全事件响应计划？
受访者百分比，N = 3,321



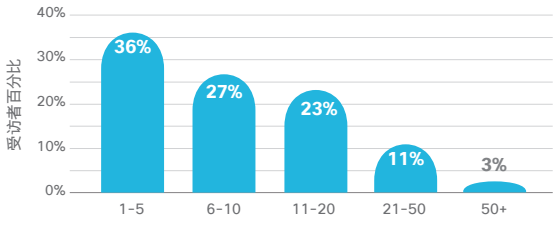
来源：思科 2019 年 CISO 基准研究报告

架构：精简供应商数量

由于对全面的网络威胁防御方法的需求日益迫切，很多组织纷纷采用了多点解决方案。2018 年，21% 的受访者拥有超过 20 家供应商，5% 的受访者拥有超过 50 家供应商。今年，这两个数字已分别降至 14% 和 3%。我们发现组织采用的供应商和解决方案数量呈下降趋势；但由于多供应商解决方案未实现集成，因此无法在有限的控制面板上共享警报分类和优先级，所以我们的调查发现，即使拥有较少单点解决方案的 CISO 也可以通过企业架构方法更好地管理警报。

要更好地管理警报，最佳安全实践是减少供应商和单点解决方案的数量。2018 年，有 54% 的受访者表示自己的环境中拥有 10 家或更少的供应商，而现在这一数字已上升到 63%（图 4）。这意味着越来越多的受访者在减少供应商数量；由于各种可能的原因，供应商整合是可行且可衡量的。

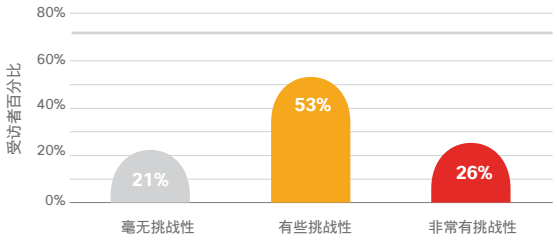
图 4 安全供应商（品牌和制造商）数量。
受访者百分比，N = 3,248



来源：思科 2019 年 CISO 基准研究报告

但是不要只听我们的一家之言。多供应商方法（而不是集成方法）导致一直以来都不曾消失的警报挑战继续存在：今年 79% 的受访者表示管理来自多个供应商产品的警报有些挑战性或非常有挑战性，而 2018 年这一数字为 74%（图 5）。因此，虽然安全专业人员正在尝试解决供应商繁杂问题及其伴随问题，但相关管理工作并未简化，需要进一步改进以优化资源。而这正是安全分析、机器学习和 AI 的用武之地，这些技术可以大力促进警报优先级和管理的初始阶段实现自动化。去年这些新技术的采用率很低，今年似乎也略有下降。

图 5 管理多个安全供应商的警报。
受访者百分比，N = 3,248



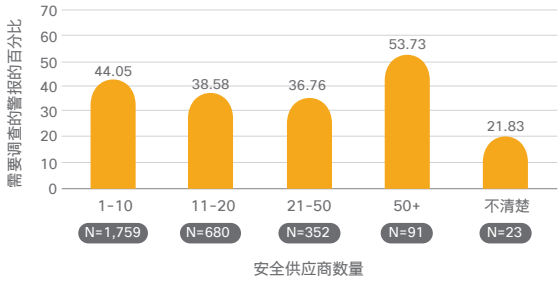
来源：思科 2019 年 CISO 基准研究报告

“如果我们能够减少供应商数量并提高架构集成性，会对我们有很大帮助。我更希望通过集成架构在后端实现更高自动化，而不是在前端强加一些东西并编写一些新脚本来将它们整合在一起。”

虽然组织的规模肯定会对警报和供应商数量产生影响，但数据告诉我们，供应商数量越少，警报管理效率越高（参见图 6）。在漏斗顶部，63% 的拥有 1-5 家供应商的组织，42% 的拥有 6-10 家供应商的组织，每天只有不到 5000 个警报。当然这也可能是因为他们关闭了一些警报。

减少必须管理的供应商的数量可以帮助您的团队专注于执行更重要的工作，例如实行补救。供应商数量少于 10 个的组织的平均响应率较高，可以对 44% 的真实警报实行补救，而供应商数量更多的组织只能对 42% 的真实警报实行补救。您可以通过减少安全供应商数量来提高效率，如图 6 所示。

图 6 安全供应商数量与需要调查的警报数量的对比。
警报，N=2,905



来源：思科 2019 年 CISO 基准研究报告

最后，我们发现 65% 的组织非常与时俱进，并且不断升级采用最好的技术，这些组织每天的安全警报数量往往较少（每天最多 10000 个）。下一个最佳选择 - 以常规节奏替换或升级安全技术（但不一定配备最新和最好的工具）- 有 60% 的可能性每天接收最多 10000 个警报。

“如果归根结底，关键都在于处理各种警报信息，这就有必要实现自动化。确保如果开始看到某种类型的事件，系统就会为我们触发事件。”

警报管理挑战：您不知道自己的盲点在何处

与从事安全工作的人谈警报数量过多，就像与大城市的人谈交通压力一样。这很让人不愉快，我们懂的，继续吧。但是，您通常会采取某些措施：拼车、避免高峰出行、在家办公。警报对于发现未知威胁也很重要，不容忽视。未知威胁占 1% 的比率，即使是最好的分层防御也无法阻止这些威胁。

以下是受访者给出的五个与警报形势相关的调查结果：

1. 受访者收到的警报数量逐年减少，这意味着要管理的警报数量更少，理论上更容易发现重要警报。警报数量最低的组织每天收到 10000 个或更少警报，59% 的组织属于该组，而在去年的调查中这一数字为50%。
2. 每天一万个警报仍然过多？确实很多，但如果考虑到 41% 的组织警报数量超过一万个并且有些组织还超过五十万个（虽然此类组织只占 1%），一万这个数字至少表示方向发展是对的。
3. 接下来就是坏消息了。50.7% 的受访者对警报做出响应，而 2018 年则为 55.6%。这表明，虽然有的组织警报数量减少了，工作似乎应变得更轻松，但实际上很多组织响应的警报数量减少了。

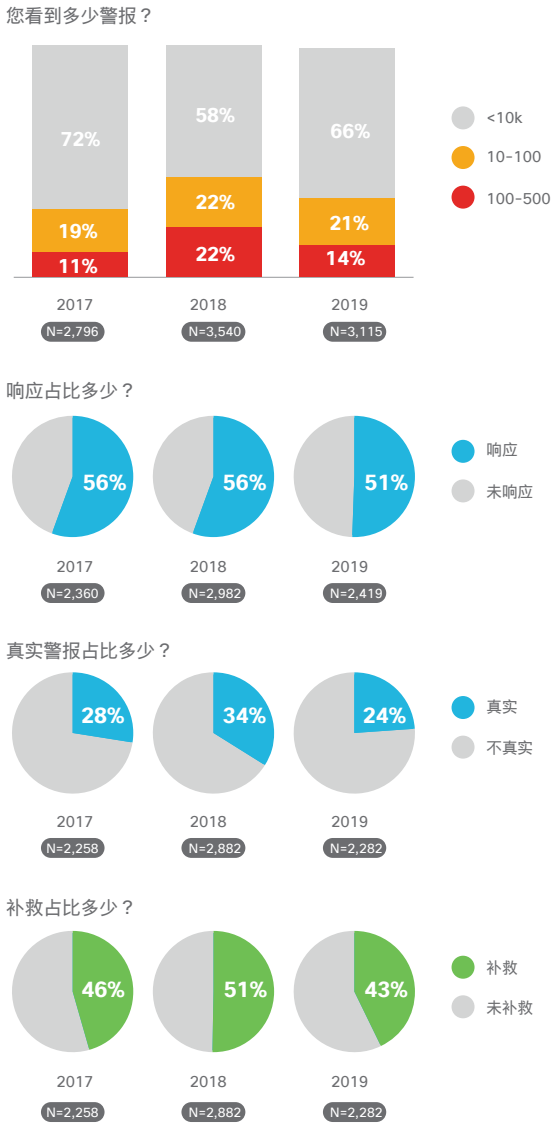
4. 经过调查的警报中，仅 24.1% 的警报是真实警报，低于 2018 年的 34%。这表明用于确定应调查哪些警报的工具的准确性并未提高。
5. 如果看一下针对警报的补救情况，会发现情况更糟糕：相比 2018 年的调查结果，今年真实警报的补救数量显著下降，从去年的 50.5% 降到了今年的 42.8%。

换而言之，如图 7 所示：如果您所在组织每天收到 10000 个警报，其中会有 1000 个真实警报未采取补救措施。每一天，您只有一半 (50.7%) 的真实警报会受到调查。对于可以提取广泛数据集、提供对大数据的可视性以及提供快速采取行动的方法的安全威胁响应工具，这种压力前所未有。

管理衡量指标

考虑到有许多人将补救措施作为安全效力的关键指标，这种补救数量的下降至关重要。使用平均检测时间作为指标的受访者平均数从 61%（2018 年）下降到了 51%（2019 年）。修复时间也从 57%（2018 年）下降到了 40%（2019 年）。最大的转变在于关注***补救时间***作为指标的受访者数量 (48%) 有所上升，2018 年为 30%。这表明安全专业人员又重新关注将补救时间作为衡量安全状况的关键绩效指标 (KPI)。*如果您将此数字与未执行补救的真实警报数量的增加、机器学习投资的减少以及培训量的缓慢上升或稳定不变相比较，可以发现，我们似乎需要在警报管理方面进行更多创新。*

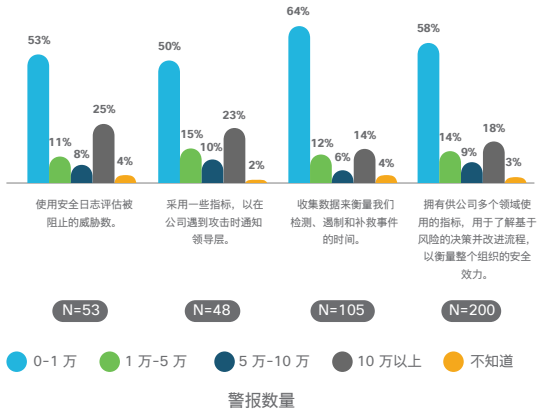
图 7 有关发现的警报数量、响应占比、响应的警报中真实警报占比以及执行补救的事件占比的调查结果比较。



来源：思科 2019 年 CISO 基准研究报告

调查数据还显示，收集数据以衡量检测时间的受访者中有 64% 每天发现 10000 个或更少的警报，这是下表中比例最高的（参见图 8）。

图 8 相比您遇到的警报数量，您的公司如何衡量您的安全效率？
受访者百分比，N = 3,259



来源：思科 2019 年 CISO 基准研究报告

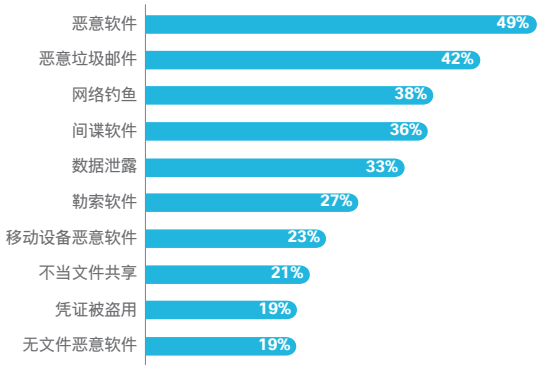
攻击应对准备和及时应对：未知威胁来临之时

去年一年之内发现的攻击

今年我们第一次特别询问了 CISO 所遇到的攻击类型，并询问了一系列常见攻击。虽然有些受访者发现了非常具体的恶意软件变体（例如 WannaCry [11%]），或威胁类别（例如 Wiper 恶意软件 [15%]），但大多数常见攻击都是恶意软件和勒索软件等变体。

“现如今，我们有 90% 的事件仍然与恶意软件，或者勒索软件和类似攻击等恶意软件的演变形式有关。而对于那些高级持续性威胁，我们还不知道威胁途径是什么。”

图 9 您在过去一年里遇到过哪些安全事件/攻击类型。
受访者百分比，N = 2,909



来源：思科 2019 年 CISO 基准研究报告

如图 9 所示，前三类中有两类是邮件安全问题；这仍然是排名第一的威胁途径。无论您是投入资金来保障迁移到 Microsoft Office 365，还是尝试使用 DMARC 更好地防范商业邮件诈骗 (BEC)，邮件都是一个需要关注的领域。前 10 类中有两类是内部威胁问题（文件共享和凭证被盗用），这表明您不仅要看到外部，还必须看到内部发生的事情，并且要注意有些犯罪分子可以合法登录而不是强行侵入。这更加突出了使用多因素身份验证 (MFA) 的必要性。

组织越来越迫切需要平衡安全需求（让合适的人员进入）与支持无缝业务（不要让笨拙的用户身份验证体验妨碍您允许进入网络的人员）。

由于其他领域仍然很受关注但可管理（例如迁移到云端），因此对用户行为的关注（例如，点击邮件或网站中的恶意链接）仍然很高，现在是 CISO 最关心的问题。对于防护基础设施各个部分时遇到的挑战，受访者最关注的是用户行为。在过去三年里，有 56% 至 57% 的受访者认为有这种漏洞，比例保持稳定。

我们还询问了哪些类型的攻击导致了某种程度的损失（数据丢失），依据受访者的回答，各类攻击排序如下：

1. 恶意软件 (20%)
2. 数据泄露 (19%)
3. 间谍软件 (14%)
4. 网络钓鱼 (13%)
5. 勒索软件 (13%)
6. 恶意垃圾邮件 (13%)

有趣的是，安全相关角色对风险的认知各异。例如，风险和合规官认为最大的漏洞是 “针对性攻击”，这些高管非常清楚致命攻击可能对业务持续性造成的严重后果。

要详细了解哪些漏洞威胁着您组织的稳定性，请阅读 2019 年思科威胁报告。

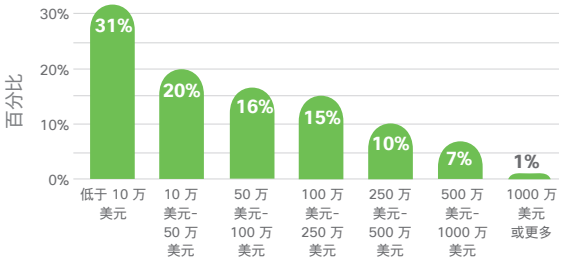
漏洞造成的损失：不仅仅是资金损失

我们都知道漏洞可能造成的后果：经济损失（参见图 10）、品牌和声誉受损或被毁、股东信心动摇、丢失有价值的数据、监管和违规处罚等。从数据的逐年比较来看，关注点明显转向了认知和情绪问题；对于保持运维的需求并没有下降，但客户体验和品牌声誉都成为了关键关注点（表 1）。

表 1 组织最关注的漏洞相关问题。

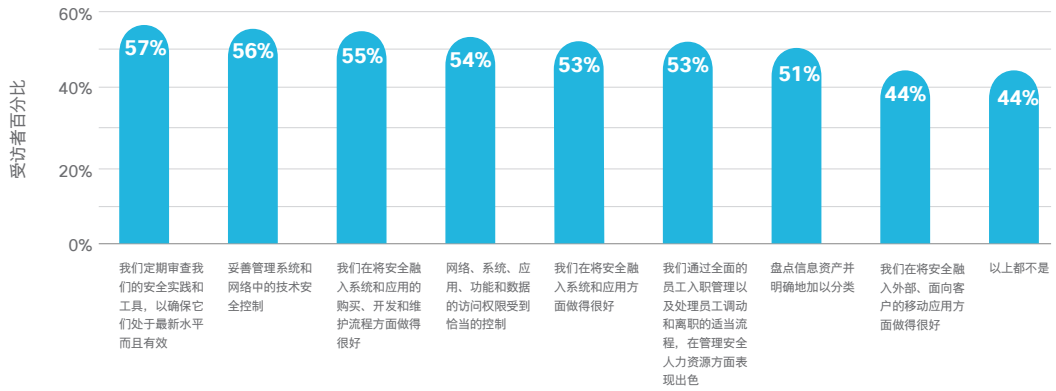
漏洞造成的问题	受访者表示：2018 年	受访者表示：2019 年	
运维	38%	36%	运维方面的担忧略有下降，但不足以弥补对留住客户的问题的担忧。
客户保留率	26%	33%	客户一直对数据泄露存在负面情绪，而且勒索软件等恶意软件的猖獗也使客户持谨慎态度。
品牌声誉	27%	32%	近年来，很多著名公司都遭到了大型攻击；在这里我们不会点名指出，但是客户非常了解此类事件。

图 10 过去一年里，您所在组织遇到的影响最大的网络攻击造成了多大财务影响？
受访者百分比，N = 2,386



来源：思科 2019 年 CISO 基准研究报告

图 11 组织采用那些实践来获得安全保护？
受访者百分比，N = 3,223



来源：思科 2019 年 CISO 基准研究报告

您采取哪些措施来解决漏洞的威胁

我们向安全专业人员询问他们的组织在多大程度上采取预防措施，将人员、流程和产品部署到位，以保护自己的组织。结果如图 11 所示。

此外，我们询问了组织采取哪些方法来降低安全风险，结果如图 12 所示。

从更多数据中我们发现，尽管 85% 的受访者对基础设施安全和保护方面的策略和实践非常了解，但只有 74% 的受访者对业务持续性和灾难恢复非常了解。**只有 75% 的受访者非常了解事件响应。这是个问题。参与安全工作的人都应该了解事件响应；事实上，这可以扩展到组织内的所有员工，所有员工都应该了解事件响应。**这使培训变得非常重要，而今年组织对培训缺乏重视的问题仍然很明显。

图 12 安全状况：为缓解安全风险而采取的方法。
受访者百分比，N = 3,248

来源：思科 2019 年 CISO 基准研究报告

应对未知威胁

发现未知威胁并采取正确行动之间的桥梁在于高效的安全评估。以下是我们根据调查结果制定的实用建议，供您参考：

- 将实用策略与网络保险和风险评估相结合，根据安全成果衡量结果编制安全预算，以指导您的采购、战略和管理决策。
- 了解业务案例的基本安全需求的唯一方法是在 IT、网络、安全和合规性团队之间开展协作。
- 组织可以采用经过验证的流程来减少遭到漏洞攻击的风险和范围。通过演练做好应对准备；采用严谨的调查方法；并且了解最便捷的恢复方法。
- ML、AI 和更高水平的自动化应该能够成倍提高安全工作效率，希望明年有更多的受访者表示“完全依赖”这些技术的实施和实践。思科的很多安全产品都利用了机器学习技术，这些产品包括高级恶意软件保护、Umbrella、Stealthwatch 和思科威胁响应等。
- 构建安全运营中心 (SOC) 来管理各种规模的组织中的漏洞响应。
- 云安全解决方案可帮助应对未知威胁。91% 的受访者认为利用云安全性可以提高网络的可视性。思科 Umbrella 是云端交付的安全产品，可确保无论用户是否位于企业网络内，都能阻止用户连接恶意域、IP 和 URL。
- 通过思科安全数据中心解决方案等集成式解决方案保护数据中心和多云生态系统，该解决方案具备 Tetration、Stealthwatch 和 NGHW 的可视性、分段和威胁检测功能。
- 通过网络钓鱼防护、高级垃圾邮件过滤解决头号威胁途径问题，并通过 DMARC 防御商务邮件入侵；了解思科邮件安全。
- 终端安全可帮助解决用户设备上的未知威胁；请尝试使用思科面向终端的高级恶意软件防护（我们的 Web、邮件、云和网络安全解决方案也有此功能），打造一个产品协同工作的环境，以实现更高效的威胁防护。
- 利用思科的网络可视性和分段功能（该功能结合了思科 Stealthwatch 企业版、思科身份服务引擎和思科 TrustSec 技术），实现快速威胁检测、高度安全访问和软件定义分段。
- 受信任的访问是保障安全的关键。Duo 使用一流的自适应多因素身份验证 (MFA) 解决方案来验证用户信任问题（确认用户是他们授权的用户）。

“有时候，应对恶意黑客，似乎就像是一场军备竞赛，但我认为对待未知威胁，我们需要关注新技术和新技术的发展方向，这样才能领先一步。”

“有时 CISO 利用恐惧心理来推动一些预算投资。我们更希望关注的是：企业面临的风险是什么？有各种可接受的风险级别，因此我们关注的是公司面临的最高风险领域。我们很幸运，思科非常重视安全，并且一直投资建设基础架构，为我们做好最充分的准备。”

Marisa Chancellor
思科安全和信任组织高级总监

思科基准调查简介

这项由独立研究合作伙伴进行的不记名调查涵盖了许多行业，包括零售业、运输业、制造业、金融服务业以及政府和高等教育行业。参与者都是在中端市场（250-999 名员工）、企业（1000-9999 名员工）和大型企业（超过 10000 名员工）组织中工作的全职员工。

受访者担任各种职务，包括首席信息安全官 (CISO)、首席信息官 (CIO) 和其他高级职务。他们通晓安全策略和程序，并参与制定安全策略。大多数人的职务是 CISO、IT 经理/主管和/或 CTO，99% 的受访者在组织中有一个致力于保护网络安全的团队。

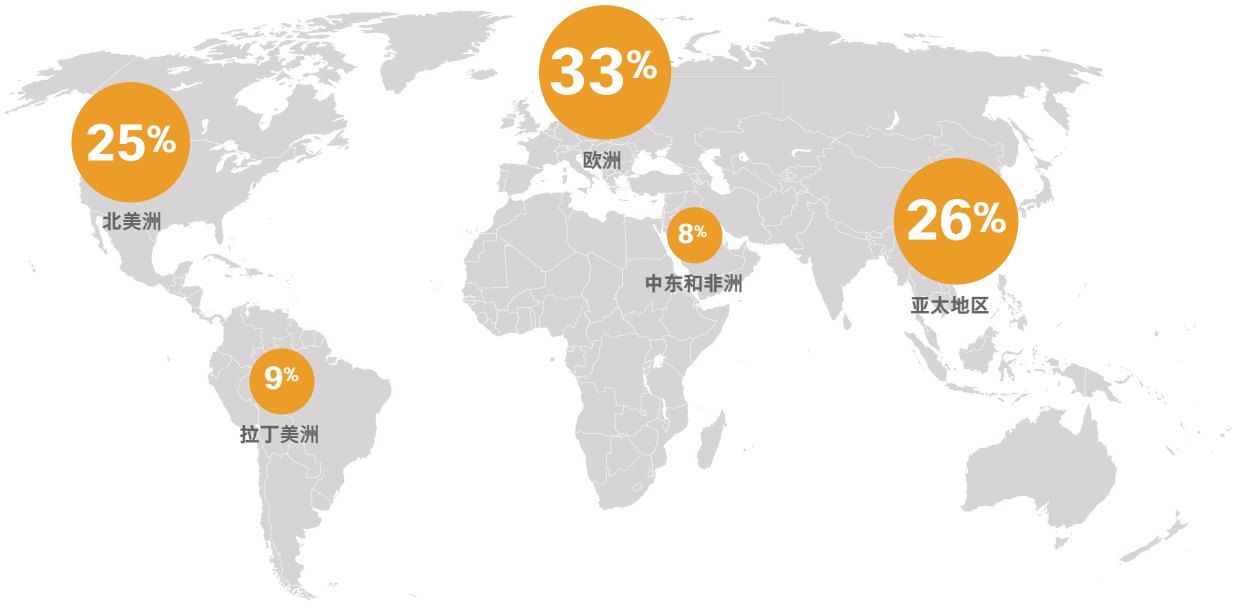
受访者来自各大洲和 18 个国家/地区，包括美国、加拿大、英国、 法国、德国、澳大利亚、日本和中国等（图 13）。

受访者选择条件

受访者需要符合以下条件:

- 通过严格筛选/竞争上岗的成年人（25 周岁或以上）。
- 在全职员工人数超过 250 人并且拥有正规 IT 部门的营利性公司、政府或高等教育机构担任全职工作。
- 参与预算核准以及其他 IT 安全工作。
- 非常了解安全策略和实践。

图 13 受访者按地区的分布，百分比经过四舍五入。
受访者百分比，N = 3,259



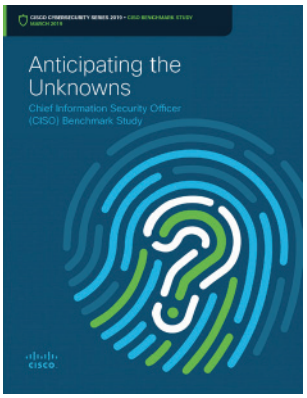
来源：思科 2019 年 CISO 基准研究报告

思科网络安全报告系列

过去十年中，思科发布了大量权威的安全和威胁情报信息，专门面向关注全球网络安全状态的安全专业人员。这些全面的报告详细介绍了威胁形势及其对组织的影响，以及防范数据泄露不利影响的最佳实践。

为了采用新方法提高思想领导力，思科安全公司以思科网络安全报告系列为主题发布了一系列基于研究的数据驱动出版物。我们进一步拓展了主题范围，针对关注点不同的安全专业人士提供不同的报告。凭借安全行业威胁研究人员和创新者渊博的专业知识，2019 年系列报告包括数据隐私基准研究报告、威胁报告和 CISO 基准研究报告，以及全年后续推出的其他报告。

有关详细信息以及要查看所有报告和存档副本，请访问 www.cisco.com/go/securityreports。



美洲总部
思科系统公司
加州圣荷西

亚太总部
Cisco Systems (USA), Pte. Ltd.
新加坡

欧洲总部
思科 Systems International BV 阿姆斯特丹
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。www.cisco.com/go/offices 中列有各办事处的地址、电话和传真。

发布日期：2019 年 3 月 CISO_01_0319_r1