实现数据隐私保护投资的最大价值

数据隐私基准研究

CISCO

执行摘要

欧盟的《通用数据保护条例》(GDPR) 于 2018 年 5 月 25 日开始实施，全球隐私法律和法规继续不断发展完善。

客户在购买周期中会询问更多数据方面的问题，包括如何获取、使用、传输、共享、存储和销毁客户的数据。

大多数组织都已经并且将继续进行人员、流程、技术和政策方面的投资，以满足客户隐私要求，并避免受到重大罚款和其他处罚。此外，数据泄露事件还在不断发生，数百万用户的个人信息遭到泄漏，组织对自己购买的产品、使用的服务、雇佣的员工以及合作伙伴和业务往来对象都高度关注。因此，客户在购买周期中会询问更多数据方面的问题，包括如何获取、使用、传输、共享、存储和销毁客户的数据。在去年的研究（思科 2018 年隐私成熟度基准研究）中，思科引入了一些数据和见解，阐明这些隐私问题对购买周期和时间进程有何负面影响。今年的研究更新了这些调查结果，并探讨了隐私保护投资的相关效益。

思科数据隐私基准研究利用了思科年度网络安全基准研究的数据，后一项研究为双盲调查，由来自 18 个国家/地区以及各种主要行业和地理区域的 3200 多名安全专业人员参与完成。本研究提出了一系列专门针对隐私的问题，2900 多名熟悉自己组织隐私保护流程的受访者对其中很多问题进行了回答。受访者回答的问题涉及他们对 GDPR 的准备情况，因客户数据隐私顾虑导致的销售周期延迟，数据泄露造成的损失以及他们当前实现数据最大价值的相关做法。

本研究的结果提供了强有力的证据，表明除了实现合规性之外，组织还从他们的隐私保护投资中获得了其他效益。相比那些尚未实现 GDPR 就绪性的组织，GDPR 就绪型组织因客户的数据隐私顾虑而导致的销售周期延迟更短。另外，GDPR 就绪型组织发生的数据泄露事件更少，并且在发生此类事件的情况下，受影响的记录数量更少，系统停机时间也更短。因此，他们由于数据泄露而遭受的总损失低于尚未实现 GDPR 就绪性的组织。尽管很多公司已着重满足隐私法规和要求，但几乎所有公司都表示，除了实现合规性之外，他们还从这些投资中获得了其他业务效益。这些与隐私保护相关的效益不断为组织提供竞争优势，同时本研究也可帮助指导组织制定投资决策，努力提高其隐私保护流程成熟度。

> **“隐私保护是组织取得成功的重要因素，既可以保护数据，也可以促进创新。”**
>
> **John N. Stewart，思科高级副总裁兼首席安全和信任官**

“这项研究证实了隐私专家长期以来的看法，即除了实现合规性之外，组织还会从隐私保护投资中获得其他效益。思科的这项研究表明，严格的隐私合规性可缩短销售周期并提高客户信任度。”

Peter Lefkowitz,
Citrix Systems 首席数字风险官，
国际隐私专业人员协会 (IAPP) 2018 年董事会主席

最终结果

59% 的公司表示他们目前满足所有或大多数 GDPR 要求，而 29% 的公司表示会在 1 年内达到 GDPR 的要求。公认的实现 GDPR 就绪性的主要挑战包括：数据安全、员工培训和满足不断发展的法规要求。

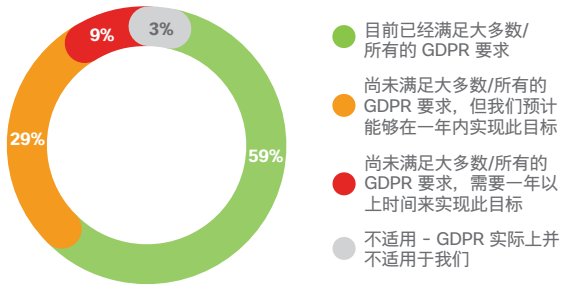
GDPR 就绪性

在数据隐私基准研究的所有受访者中，59% 的受访者表示，他们目前满足了所有或大多数 GDPR 要求。（请参见图 1）29% 的受访者表示，他们预期在一年内实现 GDPR 就绪性，还有 9% 的受访者表示需要一年以上的时间才能实现 GDPR 就绪性。虽然 GDPR 适用于欧盟境内企业或适用于处理收集到的欧盟境内用户的个人数据，但值得注意的是，在我们的全球调查中，只有 3% 的受访者表示，他们认为 GDPR 不适于他们的组织。

在不同国家/地区，GDPR 就绪性介于 42% 到 76% 之间不等。（请参见图 2）不出意料，接受调查的欧洲国家/地区（西班牙、意大利、英国、法国、德国）总体上就绪性更高。

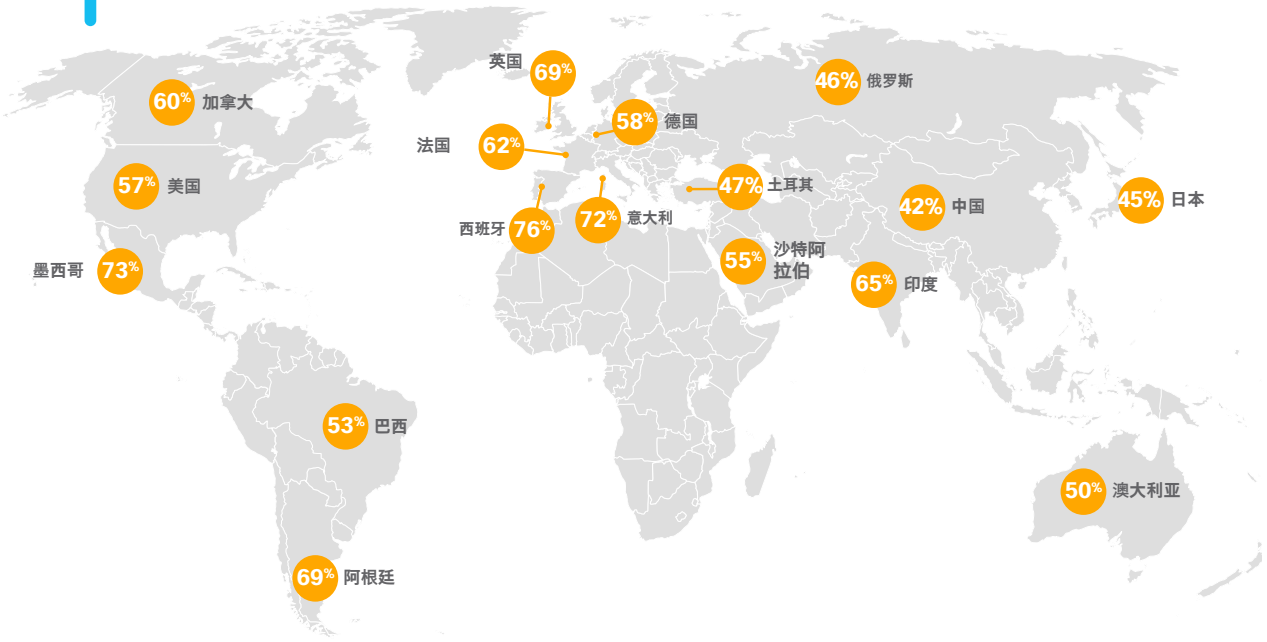
在我们的全球调查中，只有 3% 的受访者表示，他们认为 GDPR 不适用于他们的组织。

图 1 GDPR 就绪性
受访者百分比，N = 3206



来源：思科 2019 年数据隐私基准研究，n = 3206

图 2 按国家/地区划分的 GDPR 就绪性
受访者百分比，N = 3206



来源：思科 2019 年数据隐私基准研究

受访者被要求指出他们的组织在实现 GDPR 就绪性时面临的最严峻的挑战。根据他们的回答，主要挑战有数据安全、内部培训、不断发展的法规和隐私保护设计要求。（请参见图 3）

图 3 实现 GDPR 就绪性面临的最严峻的挑战
受访者百分比，N = 3098

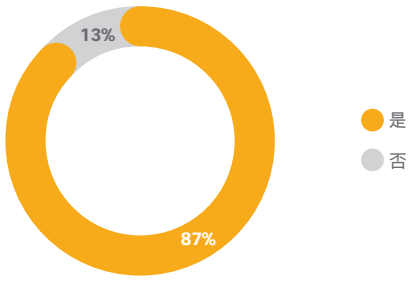
42%	满足数据安全要求
39%	内部培训
35%	随着法规的日益完善，随时满足不断变化的发展要求
34%	遵守隐私保护设计的要求
34%	满足数据主体访问请求
31%	对数据进行目录编制和清点
30%	支持数据删除请求
29%	为每个相关地区雇用/确定数据保护专员
28%	供应商管理

来源：思科 2019 年数据隐私基准研究

因隐私顾虑造成的销售周期延迟

调查向受访者询问，他们的销售周期是否曾因客户的数据隐私顾虑而出现延迟。87% 的受访者表示，确实发生过销售周期延迟，无论是现有客户还是潜在客户都曾出现过这种情况。（请参见图 4）这一比例明显高于去年的调查结果（当时报告销售延迟的受访者比例为 66%），这可能是由于人们对数据隐私重要性的意识有所提升，欧盟开始实施 GDPR，并且其他隐私法律和要求也开始出台。数据隐私已经成为许多组织董事会关注的问题，客户在开展业务之前会确保他们的供应商和业务合作伙伴能够妥善解决他们的隐私顾虑。

图 4 受访者因客户的数据隐私顾虑而导致的销售周期延迟
受访者百分比，N = 2064



来源：思科 2019 年数据隐私基准研究

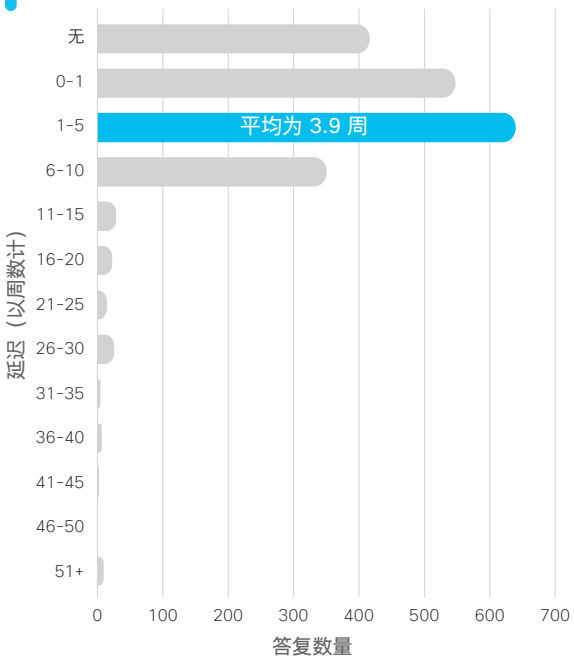
对于销售周期的延迟时间，受访者的估计结果差别很大。。现有客户的平均销售延迟时间为 3.9 周，超过 94% 的组织报告延迟时间介于 0 至 10 周之间。尽管如此，还有一些组织报告延迟时间长达 25 周至 50 周甚至更久。（请参见图 5）请注意，潜在客户的平均销售延迟时间为 4.7 周，这可能反映了在新的潜在客户关系中，组织需要更长时间才能妥善解决客户的

因客户数据隐私顾虑导致销售延迟仍然是大多数组织面临的问题。

87% **据调查，他们在向现有客户或潜在客户销售产品/服务方面出现过延迟，与去年相比延迟时间大幅增加。**

隐私顾虑。现有客户和潜在客户的平均延迟时间都明显低于去年调查报告的平均延迟时间（7.8 周），这或许反映出许多公司在过去一年中进行了更充分的准备来妥善解决客户的隐私顾虑。

图 5 因解决客户的数据隐私顾虑导致的延迟
受访者百分比，N = 2081



来源：思科 2019 年数据隐私基准研究

在不同国家/地区，现有客户的销售延迟时间介于 2.2 周至 5.5 周之间。在组织努力通过调整来妥善解决客户提出的顾虑时，如果客户的隐私要求较高或处于过渡状态，延迟时间通常会更长。（请参见图 6）

造成隐私相关销售延迟的主要原因：

- *调查特定客户要求*
- *将隐私信息翻译成客户的语言*
- *向客户介绍公司的隐私实践或流程*
- *必须重新设计产品，以满足客户的隐私要求*

图 6 按国家/地区划分的销售延迟
受访者百分比，N = 2081

国家/地区	平均延迟时间（以周数计）
阿根廷	3.9
澳大利亚	3.9
巴西	5.2
加拿大	5.1
中国	3.5
法国	4.2
德国	3.1
印度	4.9
意大利	2.6
日本	4.1
墨西哥	2.9
俄罗斯	2.5
沙特阿拉伯	4.8
西班牙	5.5
土耳其	2.2
英国	4.9
美国	3.7
整体	3.9

来源：思科 2019 年数据隐私基准研究

销售延迟至少会导致在一段时间内营收递延。这可能导致无法达成营收目标，影响薪酬、融资决策和投资者关系。此外，延迟销售往往会导致丢失销售机会，例如延迟会导致潜在客户购买竞争对手的产品或根本不再购买相应产品或服务。

调查还要求受访者指出导致其组织发生隐私相关销售延迟的原因。最常见的回答包括需要调查特定的客户要求，将隐私信息翻译成客户要求的语言，向客户介绍公司的隐私保护实践或流程，或者必须重新设计产品以满足客户的隐私要求。（请参见图 7）

图 7 造成销售延迟的原因
受访者百分比，N = 1812

49%	我们需要调查客户/潜在客户的特定/不寻常的要求，以便让他们对我们的隐私保护措施感到满意。
42%	我们需要将有关我们隐私政策/流程的信息翻译成客户/潜在客户的语言。
39%	客户/潜在客户需要详细了解我们的隐私政策或流程。
38%	我们的产品或服务需要重新设计，以满足客户/潜在客户的隐私要求。
33%	我们无法或不愿意满足客户/潜在客户的隐私要求（例如数据泄露政策、数据删除要求）。
28%	找到合适的人员或团队来解决客户/潜在客户的问题需要耗费时间。
17%	我们必须解决哪一方对数据承担最终责任的问题。
5%	我们必须让我们的律师澄清有关法律的不确定性。

来源：思科 2019 年数据隐私基准研究

隐私保护投资带来的业务效益

投资实现 GDPR 就绪性的组织主要是为了避免因不合规而遭到巨额罚款和其他处罚。但是，研究表明，这些隐私保护投资还会带来其他重大业务效益。

看一下因隐私问题导致的销售延迟，可以发现现有客户的平均销售延迟时间为 3.9 周。但是，那些表示自己满足所有或大多数 GDPR 要求的组织平均销售延迟时间为 3.4 周，尚未实现 GDPR 就绪性但预计在一年内满足此要求的组织为 4.5 周，而 GDPR 就绪性最低的组织的平均销售延迟时间达到了 5.4 周。因此，就绪性最低的组织的平均延迟时间比就绪性最高的组织几乎高出 60%。（请参见图 8）

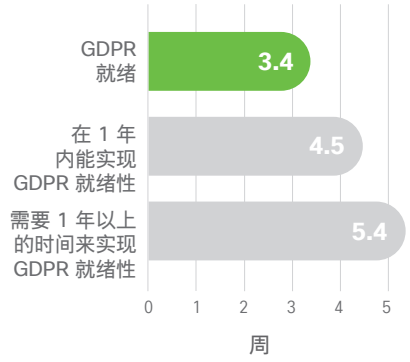
虽然大多数公司报告他们去年发生了数据泄露，但是 GDPR 就绪型公司受影响的比例最低 (74%)，相比之下，1 年内才能实现 GDPR 就绪性的组织受影响的比例为 80%，还需要一年以上时间才能实现 GDPR 就绪性的公司受影响的比例高达 89%。

主要发现结果总结

除了实现合规性之外，GDPR 就绪型公司还可以通过多种切实的方式从他们的隐私保护投资中获得其他效益。他们因客户的隐私顾虑而产生的销售延迟时间更短（3.4 周对比 5.4 周 ）。他们在去年遭遇数据泄露的频率更小（74% 对比 89%），发生泄露时，他们受影响的数据记录数量更少（79,000 条记录对比 212,000 条记录），系统停机时间更短（6.4 小时对比 9.4 小时）。因此，他们因数据泄露造成的总损失更低；去年，只有 37% 的 GDPR 就绪型公司在此方面总损失超过 500,000 美元，而 GDPR 就绪性最低的公司有 64% 遭受了此等程度的损失。

这些结果表明隐私成熟度已成为许多公司的一项重要竞争优势。组织应努力最大限度地提高其隐私保护投资的业务效益，这可能超出满足任何特定隐私法规的要求。

图 8 平均延迟周数 （现有客户）
受访者百分比，N = 2081



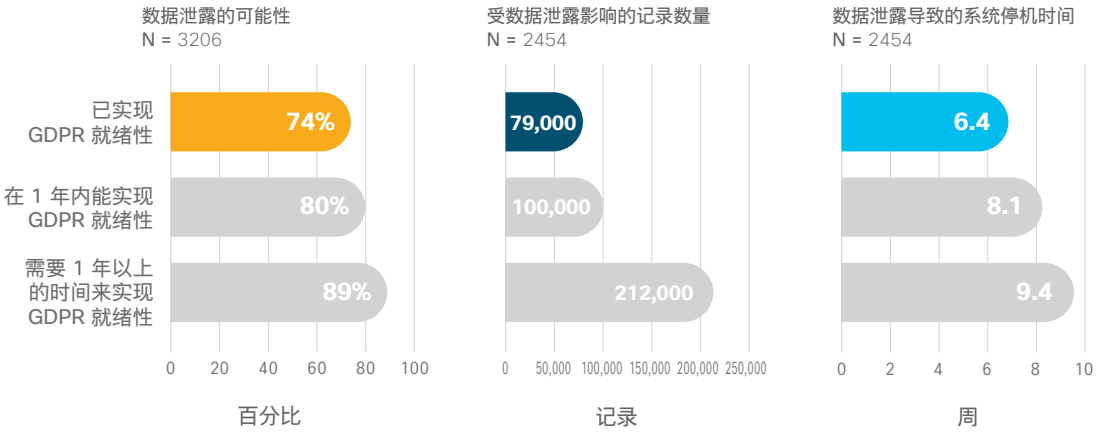
来源：思科 2019 年数据隐私基准研究

实现 GDPR 就绪性的另一个切实效益是它似乎可以降低数据泄露的频率并减少由此造成的影响。GDPR 要求组织准确掌握个人身份信息（PII）的保存位置，并为这些数据提供适当的保护。这些举措可能有助于组织更好地了解其数据以及与其数据相关的风险，并且对这些数据实施或加强保护。

> **“组织要想最大限度地发挥其隐私保护投资的价值，还有很长的路要走。我们的研究表明，数字化市场已经形成，积极进行数据资产和隐私保护投资是进入这个市场的正确途径。”**
>
> **Michelle Dennedy，思科首席隐私官**

虽然大多数公司都报告去年发生了数据泄露事件，但 GDPR 就绪型公司受影响的比例最低（74%），相比之下，1 年内才能实现 GDPR 就绪性的组织受影响的比例为 80%，还需要一年以上时间才能实现 GDPR 就绪性的公司受影响的比例高达 89%。（请参见图 9）

图 9 隐私保护投资带来的业务效益



来源：思科 2019 年数据隐私基准研究

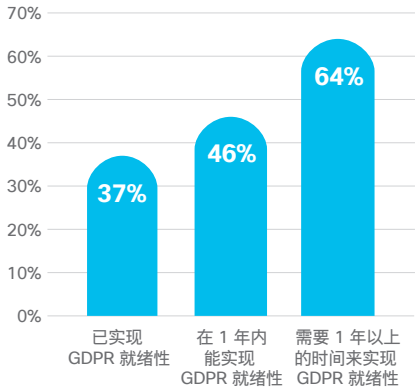
几乎所有公司 (97%) 都报告，他们目前已从其隐私保护投资中获得了其他效益，包括提高敏捷性、促进创新、获得竞争优势、提高运营效率、减少数据泄露损失、缩短销售延迟时间以及获得投资者的青睐。

此外，发生数据泄露后，GDPR 就绪型公司受到的影响更小。这类公司受影响的平均记录数量为 79,000 条，而 GDPR 就绪性最低的公司受影响的平均记录数量为 212,000 条（请参见图 9）

GDPR 就绪型公司的数据泄露相关的系统停机时间更短，这可能同样与其更为出色的数据资产管理水平有关。GDPR 就绪型公司的平均系统停机时间为 6.4 小时，而 GDPR 就绪性最低的公司为 9.4 小时。（请参见图 9）

由于受影响的记录数量更少，停机时间更短，GDPR 就绪型公司的数据泄露总损失更低也就不足为奇了。这些公司中数据泄露损失总损失超过 500,000 美元的只占到 37%，相比之下，就绪性最低的公司中这一比例为 64%（请参阅图 10）

图 10 数据泄露损失达到 50 万美元的概率
受访者百分比，N = 3206



来源：思科 2019 年数据隐私基准研究

由于发生数据泄露的记录更少以及停机时间更短，因此 GDPR 就绪型公司因数据泄露而蒙受的总损失更少。

组织认识到了隐私保护投资的效益

本研究的前两个部分强调了隐私保护投资与业务效益的相关性，例如执行此类投资的组织，销售延迟时间更短，发生的数据泄露事件更少，而且由此导致的损失也更小。值得注意的是，大多数受访者现在都认识到了其中的许多益处。当被问及隐私保护投资是否已产生效益（例如提高灵活性和促进创新，获得竞争优势，实现运营效率等），75% 的受访者指出他们获得了两种或更多效益，而几乎所有公司 (97%) 都指出至少获得了一种效益。（请参见图 11）

图 11 隐私保护投资带来的效益
受访者百分比，N = 3259

42%	通过适当的数据控制，提高敏捷性和促进创新。
41%	获得优于其他组织的竞争优势。
41%	通过整理数据和编制目录，提高运营效率。
39%	降低数据泄露造成的损失。
37%	减少因客户/潜在客户隐私顾虑造成的任何销售延迟。
36%	赢得投资者青睐。
3%	以上都不是。

来源：思科 2019 年数据隐私基准研究

报告已满足所有或大多数 GDPR 要求的组织的平均销售延迟时间为 3.4 周。

最大限度地发掘数据的价值

为最大限度地发掘数据资产在整个数据生命周期中的价值，在组织采取的整体措施中，保护数据隐私是一项关键举措。如同任何其他资产一样，组织应该有效地获取、存储、保护、利用和存档/删除数据。以适当方式最大限度地发掘数据价值的组织可以从中获益良多，不仅能赢得客户信任，还能使用受到高度保护和精心管理的数据来增强客户体验并为所有利益相关者创造更大价值。

此次调查向受访者询问了成熟数据环境中常见的一系列行为，例如是否拥有完整的数据目录，将数据与其他资产关联，雇用首席数据官以及在外部利用数据实现盈利。（请参见图 12）不到一半的受访者表示存在所有上述行为特征，这方面需要进一步研究，以更好地了解组织如何最大限度地发掘其数据资产的价值。

启示

这些结果表明，隐私保护投资创造出的业务价值已远远超出实现合规性这一初衷，并且已经成为许多公司的重要竞争优势。因此，组织应努力了解其隐私保护投资的作用，包括减少销售周期的延迟时间，降低与数据泄露相关的风险和损失，以及其他潜在的效益，例如提高敏捷性、促进创新、获得竞争优势和提高运营效率。各个组织可以将此次调查的分析和见解作为一个框架和起点，以最大限度地发掘其隐私保护投资的价值。

图 12 成熟数据环境中的常见行为。
受访者百分比，N = 3259

42%	我们了解大多数/所有数据资产的价值。
42%	我们清楚存放大多数/所有个人身份信息 (PII) 的位置以及这些信息的使用情况。
40%	我们可以有效地将不同的数据资产关联在一起，为我们的客户和我们自己创造更多价值。
37%	我们拥有相对完整的数据资产目录。
32%	我们设有一位首席数据官。
32%	我们认为自己是一家以信息为中心的公司。
30%	我们可以通过向外部销售（或交换）选择的数据来盈利。
2%	以上都不是。

来源：思科 2019 年数据隐私基准研究

以适当方式最大限度地发掘数据价值的组织可以从中获益良多，不仅可以赢得客户信任，还可以使用受到高度保护和精心整理的数据来增强客户体验并为所有利益相关者创造更大价值。

“良好的企业隐私政策可以通过为客户提供透明度和个人信息控制，保护公司免受数据泄露带来的财务损失，而有缺陷的政策可能会加剧数据泄露造成的问题。”

哈佛商业评论，“一个强大的隐私政策可以帮助公司节省数百万美元”，2018 年 2 月 15 日

总结

隐私保护投资创造的商业价值远远超出了实现合规性，并且已经成为许多公司的一项重要竞争优势。

本研究对许多与隐私成熟度相关的业务效益进行了量化。去年的报告中初步确定的许多效益已得到更充分的确认和研究，包括减少与隐私相关的销售延迟以及降低数据泄露的频率并减少由此造成的影响。在今后的研究中，我们将探讨这些效益如何随时间推移而变化，特别是随着不同行业和不同地区隐私法规和客户期望的不断发展，它们会发生哪些变化。思科将继续与我们的客户和隐私保护领域的其他领导者合作来提供信息，以便客户做出更好的投资决策并提高我们的客户信任度。

有关详细信息，请参阅：
数据隐私对业务的影响

思科网络安全报告系列简介

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。

为了以新的方式提升我们的思想领导力，思科安全部门以思科网络安全报告系列为主题，发布了一系列基于研究、数据驱动的报告。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、威胁报告和 CISO 基准研究，以及全年后续推出的其他报告。

有关详细信息，请访问 www.cisco.com/go/securityreports。

美洲总部
Cisco Systems, Inc.
加州圣荷西

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

欧洲总部
Cisco Systems International BV 阿姆斯特丹，
荷兰

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 上列出了各办事处的地址、电话和传真。

2019 年 1 月发布 PRIV_01_0119_r1