cisco SECURE

目录

简介 3

主要研究结果 5

我们有何目标？
安全计划追求的成果 7

我们采取了什么措施？
安全实践 9

我们如何实现目标？
确定成功因素 11

成功路线图 30

关于 Cisco Secure 33

附录 34

简介

我们着手编制这份研究报告，主要目标是为安全主管提供实用的工具，以指导投资，推动安全计划取得成功，并更高效地管控风险。

我们在全球开展了广泛的调查，涵盖了 25 个国家/地区和超过 4800 名受访者，旨在通过实证研究衡量哪些因素可以促进实现最优安全成果。这与我们过去创作的网络安全报告系列截然不同，我们希望这种新的方法和风格能让人耳目一新，受到大家的欢迎。

众所周知，安全形势日新月异，有时甚至会让人感觉成功遥不可及。因此，在本研究报告中我们想要解答其中一些问题：如何快速高效地管理网络安全风险？为什么即便是拥有高额安全预算的大公司，也仍难以实现某些成果？很多做法都有助于网络安全计划取得成功，安全专业人员又该着力于哪些方面？是采用新技术？还是加强培训？抑或优化事件响应程序？还有很多其他做法，不胜枚举。安全团队如何确定哪一种做法最行之有效？而且，谁又敢说这会一成不变？（提前透露一下，它肯定会变。）

本研究报告将为您提供更深入的洞察力，进一步提振您的信心，助力您抓住 2021 年及未来安全工作的重点，有的放矢。尽管过去一年可谓挑战重重，比往常更加艰难，但总是可以采取一些措施来推进安全战略。请继续阅读，了解哪些措施对您的组织最为有效。

调查简介		
抽样	**受访者**	**分析**
思科委托调查研究公司 YouGov 于 2020 年年中进行了一项完全匿名（调查发起者和受访者均匿名）的调查。	我们调查了来自 25 个国家/地区的 4800 多名在职 IT、安全和隐私保护专业人员。关于抽样调查对象的背景特征（包括所在行业、公司规模和地区），请参阅附录 A。	Cyentia Institute 代表思科对调查数据进行了独立分析，并生成了本研究报告中呈现的所有结果。
方法		
• 我们向受访者询问了他们的组织遵循治理、战略、支出、架构和运维等 25 项安全实践的情况。 • 然后，我们向他们询问了每项计划的成功程度，其中涵盖大约十几项总体性安全目标或成果，主要分为以下三大类别：促进业务发展、管控风险和实现高效运维。 • 接下来，我们进行了广泛的多变量分析，以确定与成功取得计划级别成果密切相关的安全实践。		

在报告编制过程中，我们与世界各地的很多专家（包括我们的首席信息安全官咨询团队）密切合作。看看下面一席话，相信您定会深受启发，更加迫不及待一览本报告的精彩内容。

“这份报告一定会让你爱不释手，一读再读，因为它根本不是一份让你连看都不看就随手塞入手提袋的营销报告。实际上，这份报告必将让我们对如何实施信息安全计划的认识为之一变。”

Wendy Nather，思科 Duo Security
顾问级首席信息安全官主管

主要研究结果

是否有证据表明，安全实践确实会影响计划级别的成果？

在 275 个实践与成果的组合中，有 45% 表现出显著相关性，这表明特定实践对实现特定成果的概率有影响。

其中哪个组合的相关性最强？

积极采用最佳技术的技术更新战略可让您紧跟业务增长的步伐。

哪个组合的相关性次强？

各项技术之间的紧密集成有利于吸引和留住安全人才。

希望安全计划取得整体成功？

投入资源，主动更新和集成您的技术。

想要打造一种全员支持的强大安全文化？

着力配置精良的设备，明确目标方向，提供准确的警报，并且及时修复安全问题。

希望今后能避免安全事件和损失？

对重大事件的应对措施进行事后复盘。

哪些安全实践最难实施？

在所有 25 项实践中，架构和运维类别的实践最难实施。

安全计划在哪些方面最为成功？在哪些方面存在的困难最大？

各项安全计划在满足合规性要求方面最为成功，在避免计划外工作和精力浪费方面存在的困难最大。

NIST 网络安全框架的哪项功能对安全计划取得成功的贡献最大？

就促进安全计划取得整体成功的贡献而言，身份功能位列第一，保护功能位列倒数第二。

组织是如何最大限度地降低新冠疫情对运维的影响的？

他们维护现代化的 IT 和安全基础设施，加大基于角色的培训的力度，并且持续向高管报告最新情况。

我们有何目标？安全计划追求的成果

许多安全研究（和计划）首先关注的都是具体措施，而非行动目标。但是，安全计划取得成功也不只是制定一系列目标，还要脚踏实地推动实施进程，最终才能实现目标。因此，明确我们在进程中所处的阶段，有助我们正确把握其他各项成功因素。

首先，我们确定了安全主管希望实现的一系列不同的计划层面的目标和相关成果，这是一项公认的艰巨任务。可以说，这些成果是我们梦寐以求的“终极安全目标”，尽管我们知道这个理想永远也无法完全实现。无论是安全主管还是安全计划，情况千差万别，因此我们确信，您必然会考虑根据自己的使用案例，对我们拟定的成果列表进行各种增补修改。同时，我们希望您也认同，这是一系列具有合理性和针对性的战略成果，为构建本研究的框架奠定了坚实基础。

我们要求调查受访者思考其组织在各项成果上的表现，并按照从“不堪重负”到“大获成功”的等级进行评价（如表 1 所示）。我们认识到，一些主观、抽象的概念（例如“紧跟业务需求”）可能难以理解和评分，因此我们向受访者提供了每项成果的成功示例，以指导他们进行评估（请参阅附录 B）。

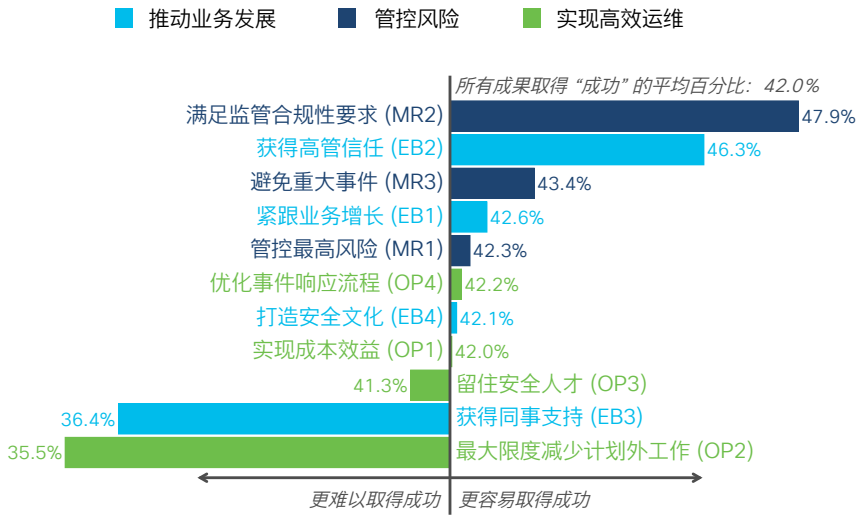
表 1：本研究中使用的安全计划成果

目标：促进业务发展	目标：管控风险	目标：实现高效运维
• 紧跟业务需求和业务增长 (EB1) • 获得高管领导层的信任 (EB2) • 获得同事和其他组织单位的支持 (EB3) • 打造全员支持的安全文化 (EB4)	• 管控组织面临的主要网络风险 (MR1) • 满足监管合规性要求 (MR2) • 避免重大安全事件和损失 (MR3)	• 实行具有成本效益的安全计划 (OP1) • 最大限度减少计划外工作和精力浪费 (OP2) • 吸引和留住安全专业人才 (OP3) • 简化事件检测和响应流程 (OP4)

在介绍了相关背景信息和限定信息后，我们言回正传，探讨手头的问题 – 参与本研究的 4800 个组织当前处于安全计划成功之旅的什么阶段？图 1 显示了声称自己的安全计划已成功实现列表中各项成果的公司所占的百分比。可以看出，大约 48% 的组织满足了合规性要求，46% 的组织获得了高管信任，如此等等，但只有 36% 的组织表示其计划最大限度减少了计划外工作。

计划级别的整体成功率为 42%，我们不禁注意到，这个结果竟然与英国作家道格拉斯·亚当斯所写的系列科幻小说《银河便车指南》里的情节不谋而合，这本小说中生命、宇宙以及任何事情的终极答案就是 42 这个数字。是巧合吗？我们认为不是，因此我们以 42% 作为整个计划成果图的基准来展示各项成果的成功率（在此值上下变化）。对于哪些成果更容易实现（靠近顶部），哪些成果更难实现（靠近底部），这种形式有助于在受访者之间达成共识。

图 1：声称所在公司已成功实现各项安全成果的受访者百分比



来源：思科 2021 年安全成果研究报告

在此图中，“保持合规性”和“最大限度减少计划外工作”呈现两极分化状态。对此，很多安全专业人员不会感到意外，因为他们认为“形式主义的监管合规性”正是安全计划效率低下的典型特征。这也从另一个侧面表明，在追求类似我们在此处列出的安全目标的过程中，组织必然会做出取舍。稍后，在确定计划成功因素时，我们将再次审视取舍的想法。

在图 1 中，各个成果类别的调查结果之间又呈现出了一种有趣的重合。显然，“管控风险”目标下的成果往往被认为难度较小，而“实现高效运维”目标下的成果则被认为难度较大。与“促进业务发展”相关的各项成果在实现难度方面则参差不齐。

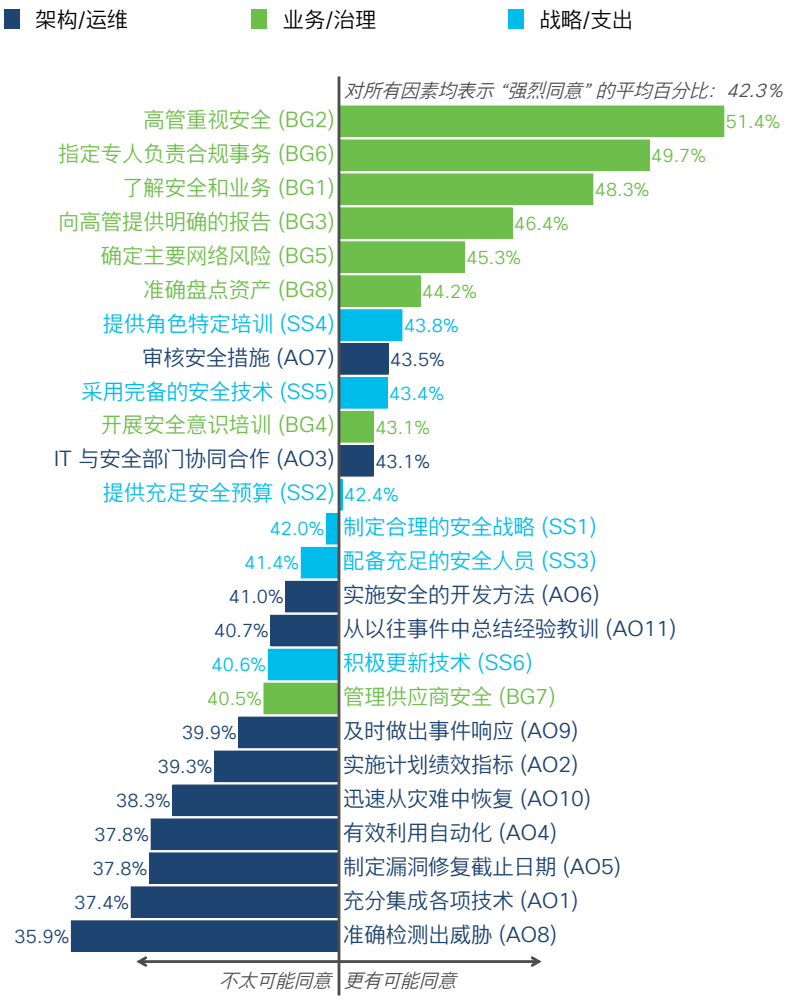
任何网络安全计划主管都深知，在最大限度降低成本的同时妥善管控网络风险，这绝非易事。如果可以选择，大多数组织都会采取规避风险的方式，通过增加支出来最大限度降低风险。

我们采取了什么措施？安全实践

接下来，我们将探讨为实现上节所述目标，组织采取了哪些措施。为此，我们向受访者询问了其组织遵循 25 项安全实践的情况。这些实践源自 NIST 网络安全框架 (CSF) 等多项标准，并且分为以下三类：业务与治理、战略与支出，以及架构与运维。与上文所述成果一样，这些实践也只是一些典型代表，在内容上无法做到详尽无遗。如需查看完整的各类别实践列表，请参阅附录 C。

图 2 对各项实践进行了排序，排序依据为受访者中强烈认为所在组织遵循了各项实践原则的百分比。我们认为图中所示的评价结果相当乐观，但我们不会对此进行深入探究，因为网络安全计划的控制措施和成熟度不是本研究的重点。我们更感兴趣的是，受访者感知到的安全实践与上节所述的他们感知到的成果之间有何关系。但是，我们暂时将这个问题搁置一边，稍后再加以讨论。

图 2：强烈认为自己公司遵循了各项安全实践的受访者百分比



来源：思科 2021 年安全成果研究报告

首先，我们要强调这些安全实践之间的相对差异。图 2 的形式与图 1 中展示各项成果的形式完全相同，也是以观察到的所有控制措施的平均实施水平 (42.3%) 为基准。顶部是受访者认为公司可以轻松实施的安全实践，而底部则是更加难以实施的安全实践。在这里，我们仅简要说明几项总体性观察结果，您可以自行分析感兴趣的具体安全实践。

我们再次发现，结果呈现出对比鲜明的极化分布趋势，揭示了安全计划多样性的有趣特征。过去，安全专业人员必须努力争取高管的关注和支持；而如今，受访者表示，这方面已经取得了长足的进步。另一方面，对于很多组织而言，业界长期实施的一些基础实践（例如威胁检测和漏洞修复）仍然是一大挑战。这让我们清楚地意识到，“夯实基础” 听起来简单做起来难。

从更广泛的角度来看，图 2 呈现出一种总体模式，即业务与治理因素位于顶部，战略位于中间，架构与运维位于底部。之所以呈现出这种模式，有更深层次的原因，而不只是 “治理容易，技术难” 这么简单。这可能反映了这些类别之间的依赖关系，也就是说，如果没有适当的治理和战略，就无法充分实现图中底部的那些实践。但是，还有一个现实是，大多数安全事件的根源都在一定程度上涉及到架构或运维问题。始终做到尽善尽美，绝非一日之功。

想要速战速决？

我们还进行了一些其他分析，比较了图 2 中所示实践的相对难度及其与图 1 中所示成果的关联。此举的目的在于，找出实施难度不大但又非常有利于促进安全计划取得成功的一些实践。如需深入了解这些易于实施的实践，请参阅我们的 #安全成果# 博客系列。

我们如何实现目标？确定成功因素

至此，我们已经探讨了安全计划的目标以及我们目前采取的实践措施。接下来，我们需要找出实现这些成果的途径。首要问题一目了然：哪些因素可以促进安全计划取得成功？

由于安全计划是一个复杂的系统，各个因素相互依赖，因此我们分析了各项实践和成果，以确定它们之间的关系。对于每项实践与成果的组合，我们计算了遵循各项安全实践的程度与实现各项成果的概率之间的变化关系。针对以下问题，我们通过这种方法得出了统计学上正确且可靠的结论：

- 是否有证据表明，安全实践实施得越有效，实现的成果也越出色？
- 哪些实践对成功取得安全成果贡献最大？
- 对于实现各项具体成果而言，哪些实践最有成效？
- 如果执行实践 *y*，实现成果 *x* 的概率会提高多少？

有些人可能觉得这些问题很简单，而且答案也显而易见。但事实真的如此？安全行业在其整体战略中采用了很多最佳实践。但是，我们并不总是去衡量这些实践的成效，并分析它们与预期成果的相关性。

的确并非如此，您是如何分析实践与成果的相关性的？

采用统计方法！读到此处，很多人可能会昏昏欲睡（或噩梦连连），但我们确实是采用严谨的统计方法进行分析的。具体而言，我们利用多变量广义线性模型来了解每项实践对每种成果的影响。也就是说，我们设计了一个逻辑回归模型，其中每个成果变量都是因变量，而所有因素都是自变量。这使我们能够测试，这些因素何时具有统计学显著性差异，何时可能只是偶然出现了相关性。

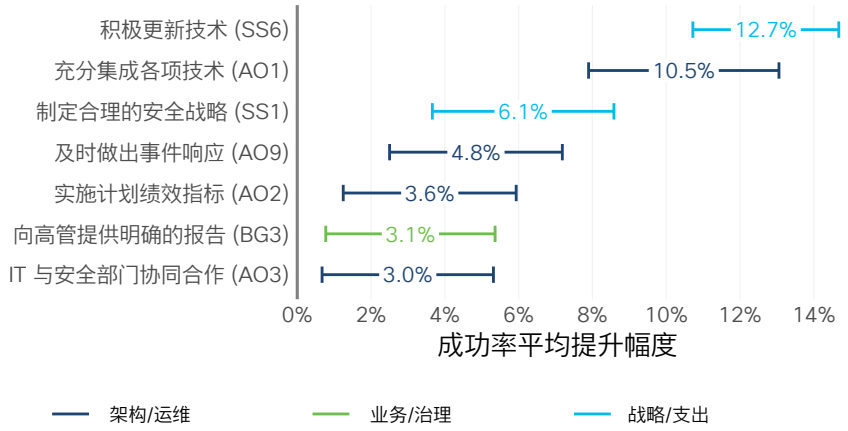
大家可能还想刨根究底，因此我们还会进一步深入分析。大家可能还记得，在逻辑回归中，各个因素的回归系数并不能直接转化为概率的变化。但是，利用“平均边际效应”这个便捷的小技巧，我们可以计算出组织可从各项因素中获得多大收益。众所周知，“相关性并非因果关系”，这句至理名言放在这里仍然适用。尽管如此，这种方法还是可以有效地彰显实践与结果之间可能有用的相关性。

计划的整体成功

首先，我们将 “计划的整体成功” 这项成果单独分离出来，因为它囊括所有其他成果。图 3 从上到下依序列出了各项因素，排序依据为各项因素与受访者表示安全计划取得很高程度的整体成功之间的相关性强弱。各条横线及相应的值表示，安全计划取得整体成功的概率随各项实践升高的幅度。由于统计差异，我们以概率范围的形式来表示这种增长幅度。中值表示计划取得成功的可能性的平均升高幅度（也是最有可能实现的升高幅度）。

这些研究结果表明，如果组织希望最大限度提高其安全计划的整体成功率，最好从采用高度集成的现代技术组合着手。一些受访者表示所在公司的技术更新战略注重使用最佳 IT 和安全技术进行主动更新，此类受访者中大多数人报告其计划取得成功的概率升高了 11% 至 15%（平均升高 12.7%）。相反，有些受访者表示所在公司很少升级基础设施或仅在出现问题时才升级，这些受访者表示其计划取得成功的概率显著下降。确保充分发挥各项技术的协同作用，形成集成化防御体系，这项实践使整体成功率平均升高了约 11%。[1]

图 3: 最有利于促进安全计划取得整体成功的实践



来源：思科 2021 年安全成果研究报告

图 3 显示了安全计划取得整体成功的概率变化范围。请像这样解读此图：“如果组织实施主动更新技术的战略，其报告安全计划取得成功的概率会提升大约 11% 至 15%，平均提升 12.7%。” 每份这样的图表都可以用这种方式进行解读。

我们深刻意识到，作为一家提供符合此类描述的技术的公司，我们会有诱导产生这种研究结果从而为自己大开方便之门的嫌疑，为此我们再次重申，执行此次调查的是一家专业调查公司 (YouGov)，参与者并不知道其中会牵涉到思科，而且执行相关数据分析的也是一家独立研究公司 (Cyentia Institute)。我们很高兴看到，这些结果验证了思科的战略和解决方案组合的重要性，但我们并未参与得出这些结论。

[1] 应该注意的是，实践与成果的各种组合的相关概率并不能累加。因此，我们不能说，如果我们主动更新技术并且充分集成各项技术，就可以使安全计划取得成功的概率提升 23.2% (12.7% + 10.5%)。

我们意识到，对于某些组织而言，主动更新技术这项战略并不总是那么容易实现。有的组织没有预算；有些组织出于各种充分的理由，需要将他们的资源和精力集中到其他方面。好消息是，这些结果并不表示此类组织处于某种失败境地。这只是意味着，他们需要确定适合自身情况的其他成功因素。这正是我们希望这种分析能够帮助他们做到的。

毕竟，拥有足够的安全预算是我们测试过的因素之一，但它与安全计划的整体成功并没有显著的相关性。因此，实现良好的安全成果不仅仅在于资金。了解了图 3 中的前两个因素之后，可以看到值得庆幸的是，制定合理的安全战略也可以带来重大优势。这是各种类型和规模的组织都可以发展的一种能力。这是其他一切实践的根本。

人们常说，危机面前方显领导者本色。图 3 表明，危机响应也是安全计划成功的一大重要因素。及时的事件响应需要进行全面的准备，配备智能工具并落实经过检测的流程。如果您需要某个合理的理由来说服自己提升这些能力，看看此图即可。

接下来的两个成功因素是相辅相成的。使用绩效指标推动运维，然后将这些指标信息明确地报告给高管领导层，这对计划的成功至关重要。这是 OODA（观察、判断、决策、执行）循环的核心，而且确实行之有效。

这就引出了最后一个成功因素，即 IT、开发和安全团队的协同合作。我们的意思不是说要开展“信任背摔”（Trust Fall，一种集体练习，一个人故意让自己向后摔倒，以便被团队其他人接住，旨在培养团队成员之间的相互信任） 之类的某种企业团建活动，而是说，此因素表明，如果您的 IT 和开发工作做得不好，就无法做好安全工作（反之亦然）。因此，完善沟通和协作，让每个人取得更大的成功，不就很合情合理？图 3 显示了在整个组织中建立强大联盟的优势。

最后要注意的一点是，安全计划取得整体成功的主要因素涵盖运维、治理和战略各个类别。这表明，安全计划的成功不能仅仅依赖于出色的治理、合理的战略或高效的运维这其中任一项独立因素，而是依赖于所有这些因素，而且越全面，成效越显著。在后续几个章节，我们将探索全部 11 项计划级别成果的成功因素，那时这个主题也将继续凸显出来。

持续升级技术与计划取得成功之间似乎存在很强的关联，而这对有些不愿意改变的组织可能是个坏消息，他们对待技术就像使用家具一样，没有坏就一直用下去。这表明“越新越好”不仅仅是从硅谷发展出来的一种生活方式，更是一种技术战略。

有关此方面信息，请参阅思科安全底线报告

NIST CSF 功能

除了遵守特定实践的情况之外，我们还询问了受访者他们的安全计划在投资、资源和工作方面的重点。为此，我们使用了 NIST 网络安全框架 (CSF) 中定义的各项高级安全功能。

就促进安全计划取得整体成功的贡献而言，CSF 的保护功能对于各项成果的贡献虽然不是最低的，但也排到了倒数第二（身份功能位列第一）。这显然违背常理，但我们认为这并不表明保护功能并不重要，而是表明最成功的安全计划应投资实施一套全面的防御体系，以对网络威胁进行识别、保护、检测、响应和灾难恢复。长期以来，业界一直高度重视保护功能，但此调查结果说明单纯依靠保护功能并不是最有效的战略。

请查看我们的 #安全成果# 博客系列，了解所有五个 NIST CSF 功能如何有助于实现计划成果。

实现安全目标

实施安全计划并取得总体成功是一个值得追求的目标，但追求特定成果也是完全合理的（而且通常是必要的）。也许您在看了表 1 中的各项成果后，会思索：“我想知道哪些因素可以帮助我们实现 [x 成果]？” 如果您有此疑问，本部分内容正好可以为您提供解答。

表中成果分为三大类：推动业务发展、管控风险和实现高效运维。在以下各标题下，我们分别介绍了几项与受访者声称其计划成功实现了每个目标最密切相关的安全实践。如果希望获得特定成果的完整成功因素列表，请耐心等待片刻，稍后报告中会为您提供一些特别信息。

以下四种实践对实现几乎每个成果都有重要贡献：积极更新技术 (SS6)、充分集成各项技术 (AO1)，及时做出事件响应 (AO9) 和迅速从灾难中恢复 (AO10)。因此，本部分的所有图表中都会频繁显示这些实践。为了获得多样化的洞察力，除了这四种实践之外，我们一般还会重点分析对于实现每项成果贡献最大的前五种实践。请不要认为这是因为我们不重视上述四种实践的重要性。有充分的理由证明，这四种实践是本研究发现的最重要成功因素。

“安全产品/服务购买者通常会购买多个供应商的数十种不同的工具，并且通常必须进行大量的整合才能使其协同工作。这会增加复杂性、成本和开销。”

Mike Hanley，思科首席信息安全官
了解详情

推动业务发展

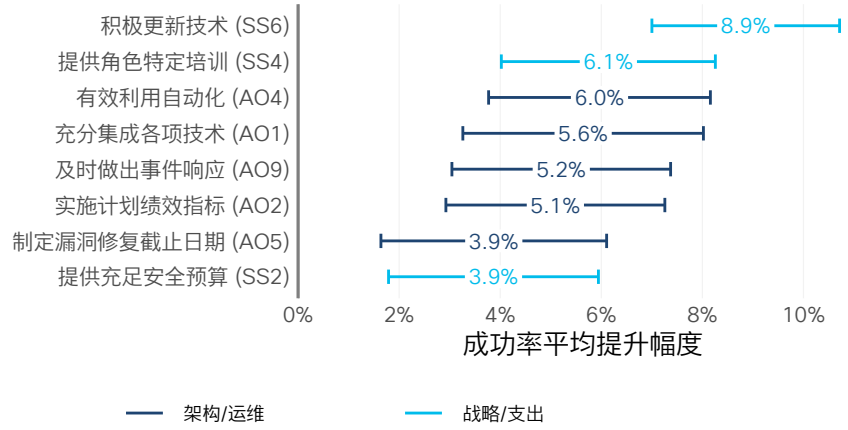
如标题所示，此部分探讨的成果侧重于安全计划对业务活动的支持和促进作用。此类别确认了实施安全计划不只是为了保障安全，它还可以促进业务发展。让我们一起探索是否可以找到一些实现这一目标的秘诀。

紧跟业务需求和业务增长

频繁升级采用最佳可用技术，并集成这些技术以使之密切协同工作，这两种实践在图 4 中再次占据突出地位。由于我们已经对这些实践进行了充分讨论，我们将不再赘述，只是简要地说明这一调查结果对我们来说非常有意义。“紧跟业务发展” 这整个理念要求安全计划必须随着创收活动一起迁移、改变和调整。任何想要通过旧技术实现新发展的人都知道，这几乎是不可能的。东拼西凑的过时基础设施只会阻碍业务发展。

针对特定角色的安全培训可以显著促进业务发展，对于这种关联我们颇感欣慰。实际上，我们将其融入了我们的准则，即 “培养优秀人才，实施敏捷计划”。有些人可能会说，这是现代安全计划中最基本的主题之一。有效的培训必须保障卓越的成效，符合企业文化，并为特定受众量身定制。

图 4：对紧跟业务发展贡献最大的主要安全计划成功要素 (EB1)



来源：思科 2021 年安全成果研究报告

将自动化纳入图 4 中，对我们也很有意义。自动化可以消除瓶颈并提高人员、流程和技术的敏捷性，帮助安全计划紧跟业务发展。图 4 凸显了技术现代化、自动化和集成的重要性，这开始呈现出明显的 DevSecOps（开发、安全与运维）特征。

乍一看，事件响应 (IR) 被列为首要业务推动因素似乎有些奇怪。但是，事件响应并不仅仅是应对紧急事件和收拾残局。它的最终目的是，在尽可能降低对业务的影响的情况下，妥善处理意外事件。因此，在图 4 中列出这一项就完全合情合理。

从表面上看，指标驱动的安全计划旨在根据不断变化的情况调整方向。我们认为，性能指标之所以被视为有助于促进安全计划紧跟业务发展的步伐，这就是其原因所在。如果您不确定自己所处的阶段或追求的目标，行动再快也无济于事。

毫无疑问，拥有充足预算可以促进安全计划紧跟业务发展的步伐。这一点值得谨记，尤其是在您的业务模式涉及速战速决和快速发展的情况下。在安全方面进行适当的投资可以帮助推动这一发展势头。

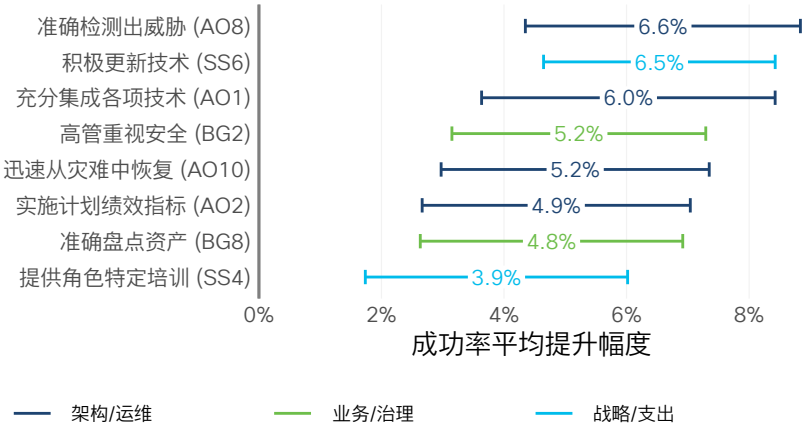
点击此处，了解思科首席信息安全官如何通过安全计划推动业务发展。

获得高管领导层的信任

集成现代技术，又可以带来一项优势。说到这里，我们不禁会想到高管视察安全运维中心的情境（突然就想赶紧清理办公桌，摆出忙碌的样子），但至少有一些证据表明，这种 “技术视察” 确实有效!

许多企业高管将网络安全计划视为一种保险，用以防止其公司由于重大网络攻击或业务中断而见诸报端。在与赢得高管信任相关的因素当中，准确地检测出威胁和迅速从灾难中恢复名列前茅，而上述担忧可能就是其背后的原因所在。能够展现出强大的可视性和恢复能力，就能够向领导层传达我们的安全计划卓有成效。

图 5：有助于获得高管信任的首要安全计划成功因素 (EB2)



来源：思科 2021 年安全成果研究报告

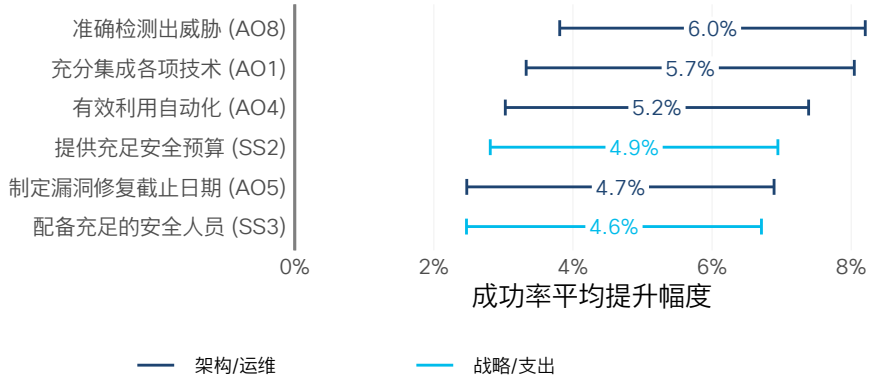
提供准确的资产清单，制定计划绩效指标并针对特定角色进行培训，似乎依然是为高管排忧解难的良方。展示安全团队知道企业的重要资产所在，具备保护这些资产的技能，并且跟踪可靠的指标以证明其安全计划确实卓有成效，这些实践都有助于赢得高层信任。

高管重视安全，自然就会更加倚重安全团队。这可能是 “相关性并非因果关系” 这条格言的一个良好例证。如果他们重视安全，就可能会为安全计划提供充分的支持，做出更多投入来促进其取得成功。

获得同事和其他组织单位的支持

我们已经看到并讨论过图 6 中所示的几个主要成功因素。但还是可以再看一下，良好的安全运维（即检测、集成和自动化）有助于赢得其他团队/部门的尊重和参与。甚至可以说，良好的安全运维依赖于这些团队。这些实践可以减少障碍，增加灵活性，并且通常可以帮助安全计划摆脱“无所作为”的耻辱。

图 6：有助于获得同事支持的首要安全计划成功因素 (EB3)



来源：思科 2021 年安全成果研究报告

说到耻辱，安全相关的支出经常会影响 IT 和开发组织的预算（有时候这种影响会超出对方可接受的范围）。因此，给安全计划单独提供充足的预算，可以帮助安全计划赢得同事的支持。同样，配备充足的安全人员也有助于赢得同事的支持。原因是，如果其他部门不需要为参与安全计划消耗自己的预算或占用自己的人员，那他们肯定会参与，而且还会心怀感激。

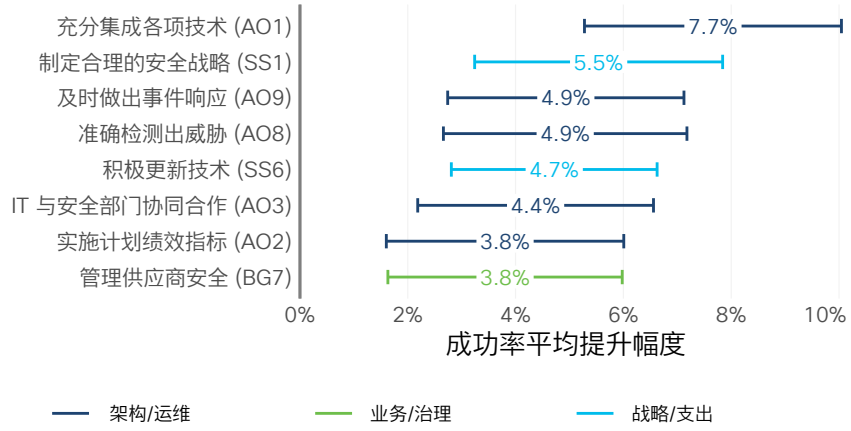
漏洞补救是上文所述情形的一个具体示例。如果没有 IT 团队和安全团队之间的协作，就很难做到这一点。安全部门经常会发现漏洞，而 IT 部门可以实施补救。显然，协调各个部门各尽其职，可以促进部门之间的同事协作。

打造全员支持的安全文化

如何打造一种真正受到全员支持而不是回避的安全文化？图 7 将以下因素放在首位，即：为员工提供满足其需求的先进技术，树立明确的方向感，及时修复问题（或者首先积极防范问题）。这些措施都是不言而喻的，不容辩驳。

安全文化并不仅仅意味着要开展培训，尤其是那种一年一度的在线安全意识培训，人人都深恶痛绝。当然，这也不意味着“只要你违反安全政策，我们就会要求你再次完成相应培训，以示警戒。”特别值得指出的是，战略与文化的相关性。这是在“促进业务发展”类别下，唯一一个可以通过制定合理的安全战略来显著提升成功概率的成果。这看起来很奇怪，但不妨考虑一下实施新安全战略时的情况：很多员工可能会很沮丧，询问“我们为什么要经受这些事情？”而实施一个合理的战略，可以让大家达成共识，从而消除他们的这种沮丧。

图 7：打造强大的安全文化的首要成功因素 (EB4)



来源：思科 2021 年安全成果研究报告

前面我们已经看到，IT、开发和安全团队协同合作有助于计划取得总体成功，而且这种合作无疑也有助于发展企业文化。安全计划不能靠强制实施，而必须融入基础设施架构和组织本身当中，才能真正产生成果。技术团队之间的密切协作对于实现这一目标至关重要。

图 7 中还包含“管理供应商安全”，这让我们有点疑惑。然而，通过受访者对相关问题的回答，我们可以从中窥见一斑，受访者表示：“我确信，我的组织价值链/供应链中供应商的安全实践符合我们的标准，或者我们可以相应地进行管理。”我们认为，从中我们可以合理推断出来，如果公司将安全计划扩展到其整条供应链，就更有可能同时将安全渗透到自身企业文化中。

SECURE

安全案例

思科采访了 Elevate Security 联合创始人 Masha Sedova，详见我们的安全案例播客。

聆听这一期激动人心的视频，了解如何通过使用数据和分析功能在公司的网络安全方法中引发文化和行为变革，通过员工推动实现网络安全。

详情请访问 cisco.com/go/securitystories。

管控风险

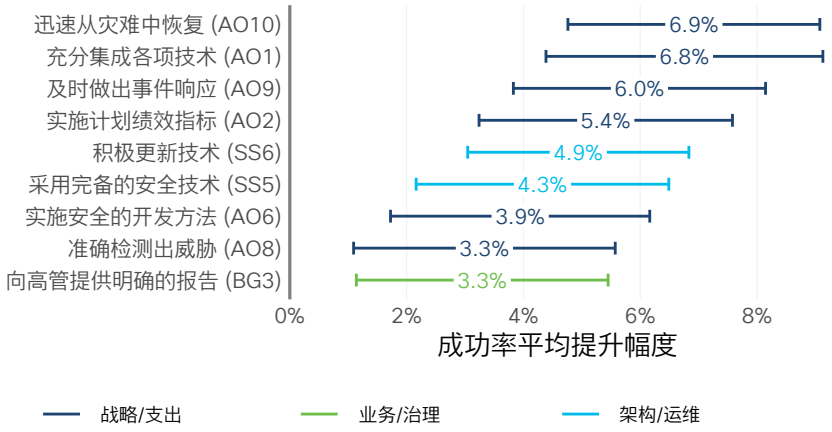
在被问及安全计划的主要作用时，大多数人想到的都是管控风险。当然，风险是多方面的，因此我们选择分析三个成果，每个成果都为探索组织如何管控风险提供了一个独特视角。

管控组织面临的主要网络风险

我们存在对一些小细节解读过度的风险，例如在图 8 中，“迅速从灾难中恢复”位列前茅，超过了“积极更新技术”和“充分集成各项技术”这两个因素。但是，相关数据可能揭示了一些重要信息，并且提醒我们，管控风险并不仅仅是防止发生不良事件。同样重要的是，在不可避免发生事件的情况下将影响降至最低。这就是迅速从灾难中恢复的意义所在。

只有两个成果可以通过采用完备的安全技术和积极进行更新取得显著成功，灾难恢复便是其中的成果之一。我们认为这是因为，相关数据进一步证实，配备最佳工具并使之保持最佳状态是管控关键风险的最有效措施。

图 8：有助于管控主要风险的首要安全计划成功因素 (MR1)



来源：思科 2021 年安全成果研究报告

一直以来，我们都注重采用安全指标，我们很高兴看到实施数据驱动的安全计划可以改进风险管控。“无法衡量，就无法管控”这句话都被用烂了，但依然非常有道理。它适用于许多方面，包括网络安全领域。

我们很惊讶地发现，“管控风险”是唯一与安全的应用开发方法密切相关的成果。但是这也在情理当中，因为软件漏洞是许多网络风险的根源。

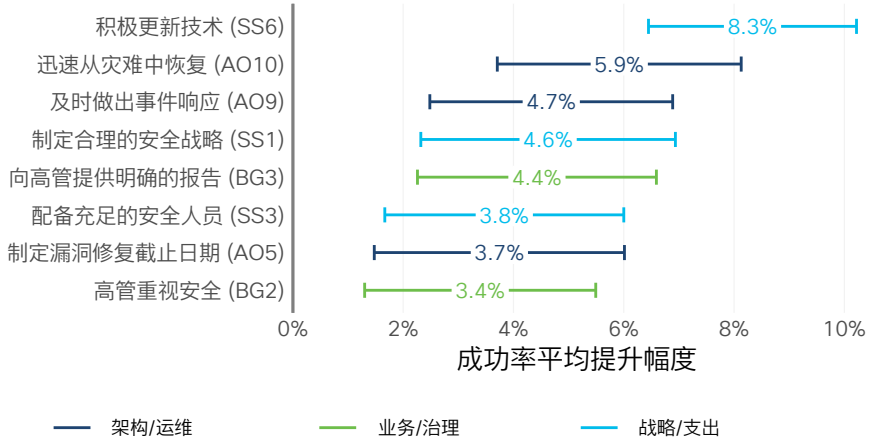
同时，这也第一次证明了向高管提供明确的报告至关重要，对此我们应该展开来分析一下。只是向领导层报告安全计划的活动和成效，就会有效地降低组织面临的严重风险，这值得怀疑。话虽如此，但这种做法确实意味着某种程度的监督和问责可以促进落实安全计划，实现切实成果。当然，我们可以看到，它就相当于绝地武士的控心术，无形之中向领导层证明了：“瞧，这就是你们需要的成果保障；我们的计划成效显著。”

满足法规合规性要求

在本文的各图表中，“积极更新技术”一直位列前茅，但在促进满足合规性要求方面，它也具有领先地位，就有点让人捉摸不透。出色的现代化解决方案是否有助于满足一系列合规性要求，并且创造卓越的审计跟踪结果？我们并不完全确定，但肯定需要注意这一点。

图 9 中的几种实践可视为有力的证据，它们可以证明安全计划涵盖了一些充分有效的措施，包括：制定合理的战略，及时补救漏洞，快速对事件做出响应，并迅速从重大事件中恢复。这些措施非常有助于保持合规性。

图 9：促进满足合规性要求的主要安全计划成功因素



来源：思科 2021 年安全成果研究报告

高管深刻意识到了法律和监管的风险，因此在董事会级别的安全报告中，这个主题一直是他们关注的头等要务。关于此图表中包含的“向高管提供明确的报告”，如果安全主管能够向企业高管清晰阐述安全计划的状态和成效，那他们同样也可以向监管机构报告这些信息。或者，获得了这些报告的高管也能够更好地与监管机构沟通，从而帮助实现合规性。

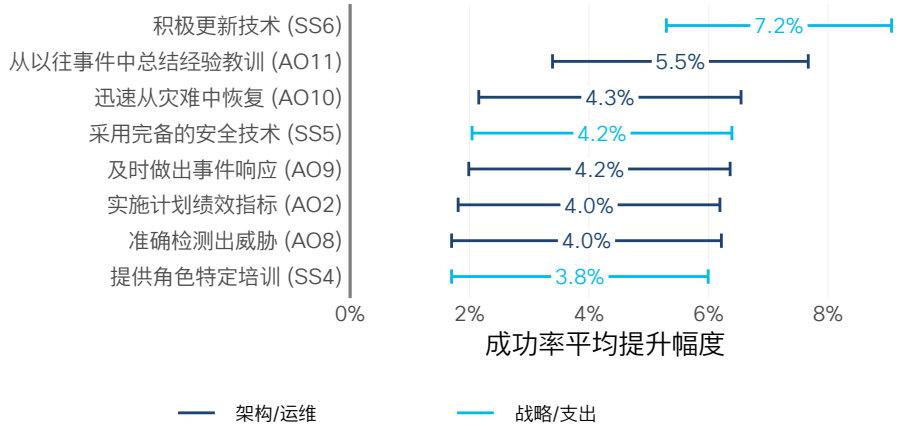
前面我们没有讨论与实现成果不相关的实践，但“向高管提供明确的报告”这种实践不能忽视。我们分析了若干因素，其中一项是从员工中指定一个人负责合规性事务。但是，这种做法并不能提高任何成果的成功概率，对于这项成果也是如此。诚然，仅仅设置一个负责合规性事务的岗位并不足以达到监管机构的要求。然而，如果说指定专门的负责人有助于实现任何目标的话，那就是满足合规性这个目标了。

避免重大安全事件和损失

在我们看来，图 10 清楚地表明，“攻击者一直在翻新花样，因此我们也必须积极变革”。能否避免重大网络安全事件和损失在很大程度上取决于维护成效卓著的现代化 IT 和安全基础设施，并辅之以灵活的响应和恢复功能。

积极更新技术战略的一个附带优势是，技术系统会得到定期检查，而不是被遗忘，直至过时。纵观各种重大漏洞事件的历史，很多事件都是由于组织忽视、未及时更新或没有以其他方式密切维护各种系统，让攻击者得以入侵其环境并建立据点。基础设施陈旧不堪，恶意攻击者就可以轻松入侵并顽固驻留在其中。

图 10：有助于避免重大事件的主要安全计划成功因素 (MR3)



来源：思科 2021 年安全成果研究报告

说到漏洞攻击的历史，图 10 表明，要了解如何避免这些事件，我们不应该只是研究大型公共事件，还应该分析我们自己遇到的事件（以及只是侥幸逃脱的事件）。在发生重大事件之后，进行事后复盘，并牢记这些经验教训，形成这样一种安全文化，可以更充分地应对未来事件。

除了帮助管控主要网络风险外，性能指标还可以提高安全计划规避漏洞攻击的几率。再加上准确地检测威胁，二者结合可提供全面的情景感知。了解攻击者的能力和活动以及您自己的防御能力和活动，有助于打破在安全斗争中组织所处的不利地位。

最后但并同样重要的是，针对特定角色的培训可以提高计划避免重大事件和损失的能力。为了正确理解这一点，可以看到调查数据显示，在最大限度地降低漏洞风险方面，培训与威胁检测一样有效。现在，哪个实践在您的组织中获得了更多资金？培训是为取得成功而经常提出的必要措施之一，但在预算紧缺时，培训往往是最重要的措施之一。如果您需要证据来向您的组织领导层证明投资培养员工最符合他们的利益，请参阅此图表。

重大事件和损失聚焦

发生重大安全事件或丢失数据并不意味着安全计划的失败（未发生此类事件也不能证明安全计划就是成功的），然而无疑，重大事件和损失是组织领导层关注的首要指标。有的受访者表示其公司在避免安全事件方面举步维艰，为此我们询问了这些受访者，请他们进一步阐述他们在此方面存在的困难。他们报告的最常见的安全事件类型为数据泄露、勒索软件和服务中断。

我们也希望了解这些事件的影响。最常见的是对运维的影响，这显而易见，因为重大事件会迫使人员（和系统）停止正常业务活动，以应对相应事件。其次是监管处罚，还有品牌损失、业务关系受损、收入损失，以及遭受法律诉讼。有关事件和损失的更多详细信息，请参阅 #安全成果# 博客系列。

实现高效运维

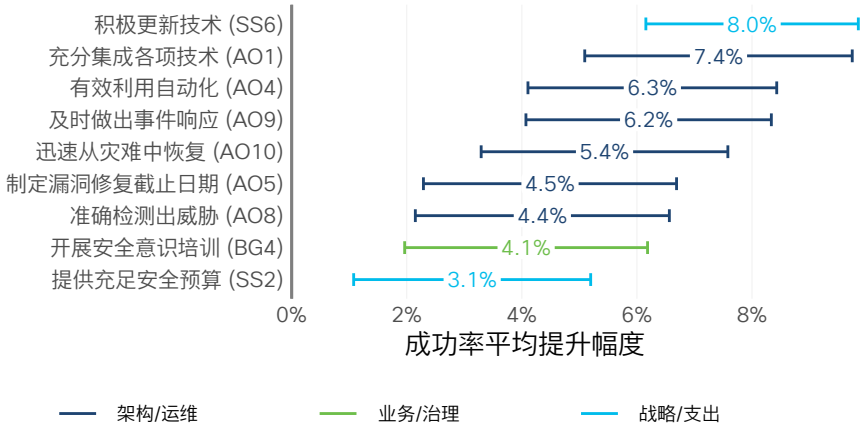
除了促进业务发展和管控风险之外，实现高效运维也是成功的安全计划与普通安全计划的区别之一。在我们的研究报告中，最后一组成果涉及成本效益、执行战略、人才管理和事件响应流程。这些都很重要，对吧？让我们来看看，如何为您的计划提供优势。

实行具有成本效益的安全计划

乍一看，积极更新技术的战略居然有助于安全计划实现成本效益，似乎有点违背常理。但是，我们之前说过，技术更新不只是让安全人员单独受益。这种战略可以确保您的整个团队拥有最佳工具，从而助力他们发挥最大潜能。此外，如果您的安全工具未保持最新状态，您就很难执行图 11 中的后两种实践（集成和自动化）。从长远来看，工具越先进，成效越显著，越易于管理，因此成本就越低。

图 11 中的后两种实践，我们也已经多次看到它们。如果您遇到过重大安全事件，您就会知道，响应和恢复过程可能会花费大量时间和金钱。确保充分实现技术集成和自动化，在必要时及时应用这些技术，可以同时遏制事件损失和相关成本。

图 11：有助于实行具有成本效益的安全计划的主要成功因素 (OP1)



来源：思科 2021 年安全成果研究报告

在安全任务中，没有什么比漏洞管理和对海量误报进行甄别更令人沮丧的了。因此，依据我们的分析，在图 2 所示的组织充分实现的实践当中，这两项功能处于垫底位置，就不足为怪了。这两项功能难以实现，而且会消耗大量资源。值得庆幸的是，图 11 显示制定补救截止日期和准确地检测威胁可以提升计划成效，这为疲于应对漏洞管理与误报的人带来了希望。

在为此成果分配安全预算方面，需要遵循适度原则。太少了，无论您如何努力，都无法完成各项任务。太多了，就会造成浪费。但是，如果预算不多不少，正正好，那么计划的各项功能就可以与安全任务完全契合，实现最高的运维效益。

总体而言，通过合理设计安全架构并辅之以高效的运维，可以使安全计划最轻松地实现成本效益。

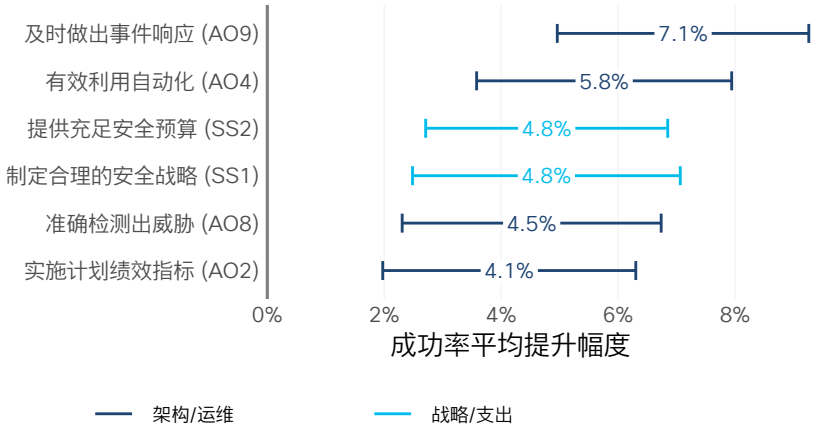
最大限度减少计划外工作和精力浪费

此成果与实行具有成本效益的安全计划相似，但更多地侧重于执行战略，避免重大失误或偏差。因此，首先制定良好的战略可以使前五种实践发挥作用，推动实现此目标。准备足够的预算来实现此战略也有很大帮助。

图表中的其他因素（及时响应、有效的自动化和准确的威胁检测）为该战略的日常执行提供了先发优势。威胁检测和响应不力尤其容易造成阻碍。如前文所述，不顺畅的事件响应流程和海量的误报甄别工作会导致时间浪费，使员工精疲力尽，并且造成很多其他得不偿失的影响。安全自动化和协调的主要目的是消除运维的死角和瓶颈。值得庆幸的是，这样确实行之有效。

对于实现此目标，同样重要的是性能指标，它可以暴露安全计划的方向问题，并为确定安全计划何时偏离正轨提供了衡量工具。

图 12：有助于最大限度减少精力浪费的主要安全计划成功因素 (OP2)



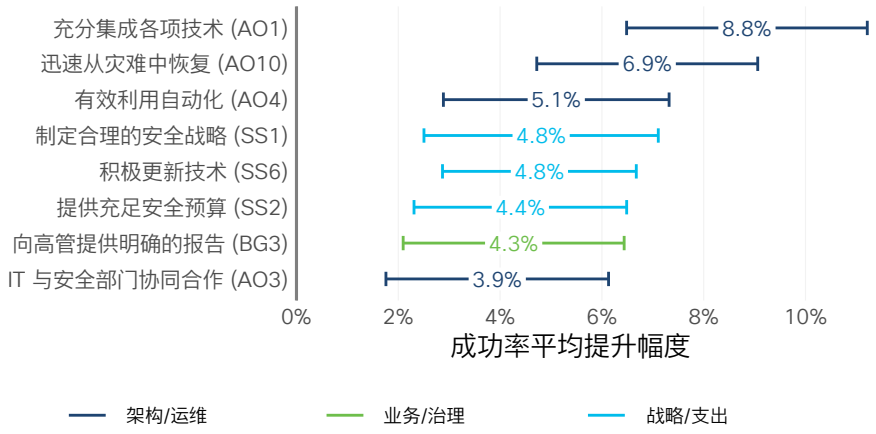
来源：思科 2021 年安全成果研究报告

吸引和留住安全专业人才

在吸引和留住安全人才方面存在的各种困难，一直是业界非常关注的话题。有一种方法或许会有所帮助，即：安排预算以聘用顶尖人才，制定他们认可的战略，为他们配备优秀的同事，并为他们提供成功所需的工具。人才的多元化及其背景、技能和观点对于创造一种让员工感受到包容、尊敬并积极寻求职业发展的企业文化至关重要。

说实话，图 13 中列出的实践主要都侧重于技术因素，有点让我们出乎意料。我们原本以为，这个方面的成功因素技术性会弱一些。但是，一如既往，面对相关数据，我们不得不改变我们的想法。经过一番思考，我们承认，架构和运维在吸引和留住高级安全人员方面作用举足轻重。这是因为，绝对没有人喜欢浪费时间和才能来克服低劣技术造成的问题。

图 13：有助于留住安全人才的主要成功因素 (OP3)



来源：思科 2021 年安全成果研究报告

关于减少时间浪费和留住人才的问题，安全自动化是一个值得一提的应对措施。有些人将自动化视为一项替代人力的措施，但是了解如何善用自动化的人深知，自动化的作用在于减轻人才工作负担，而不是替代他们。通过减轻员工的日常工作负担，就可以让他们有更多的时间去从事更具挑战性、更有趣味和价值的工作。这些调查结果表明，安全专业人员对此非常认同。

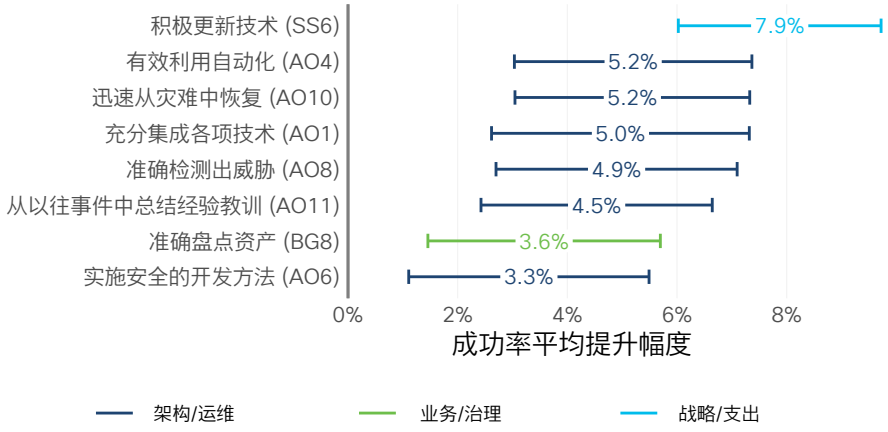
IT 团队和安全团队密切合作，是另一个值得一提的成功因素。要打造这种协作文化并非易事，但出于许多原因，依然值得去尝试。图 13 表明它还有助于留住人才，这为组织努力打造协作文化提供了又一个充分的理由。

实现网络安全的途径不止一个。在这本题为网络安全的多样性：安全行业职业的无限可能的电子书中，我们采访了多位著名的网络安全专业人员，以揭示他们是如何开始步入这个行业的，并邀请他们分享了对年轻同行的建议。

简化事件检测和响应流程

与很多其他成果相比，最后这个成果战术性更强，而且从类别上看它与 “及时做出事件响应” 这个实践存在重叠。但是，通过查看附录 B 中对此目标提供的说明和例证，可以发现优化事件响应既是一个目标，也是一个手段。此外，与事件响应同样重要的是，威胁检测和其他核心安全运维 (SecOps) 实践也是有助于实现本节所述成果的成功因素，因此我们需要思考如何改进这些功能。

图 14：有助于优化事件响应流程的主要安全计划成功因素 (OP4)



来源：思科 2021 年安全成果研究报告

一部分答案在于采用经过调整优化的现代安全架构，并辅之以成熟的运维，这种方法我们在此研究报告中经常提及。至此，我们可以说这是实现网络安全的必备条件。我们更关注的是，要想取得成功，还必须满足什么其他要求，从图 14 所示的最后三项因素可以窥见一斑。前面我们已经提到过一次 “从以往事件中总结经验教训” 的重要性（对于避免重大事件和损失而言），很高兴在这里再次看到了这个成功因素。虽然其重要性不言而喻，但是您可能会很惊讶，有很多事件响应团队并不愿意花时间真正来做这件事。只有两个成果可以通过准确盘点资产取得显著成功，而 “从以往事件中总结经验教训” 便是其中之一。如果您听到过这种声音，“我们都不知道那台（受感染的）服务器还在用”，以及 “我们不确定那个应用程序在什么位置”，就会发现 “准确盘点资产” 与 “从以往事件中总结经验教训” 具有多么紧密的关联。如果您不知道资产位于何处，归谁所有，其配置情况如何，就很难做出有效响应。

在力求证明采用安全的开发生命周期的合理性时，人们通常不会想到优化事件响应流程。但是，采用这种实践可以通过 DevSecOps（开发、安全、运维）促进安全和开发团队/流程实现更紧密的融合。这反过来又可以提升应用的性能和恢复能力，使大家对受攻击面达成更深入的共识，提高对漏洞以及问题应对措施的认识。

降低新冠疫情的影响

我们向调查参与者询问了新冠疫情对于他们的组织的影响，这个方面可以纳为 “实现高效运维” 这个类别的另一个成果。成功地将新冠疫情对其运维和网络风险状况的影响降至最低的公司具有以下特征：

1. 他们制定了积极的技术更新战略，注重不断升级采用最佳 IT 和安全技术。
2. 他们拥有足够的安全人员，并通过基于角色的培训计划着力培养员工。
3. 他们坚持向高管层明确报告安全计划的活动和成效。

通过分析这些结果，我们认为组织从新冠疫情这样的意外事件中恢复的能力在很大程度上取决于他们是否采用性能卓越的现代技术，培养优秀人才来发挥这些技术的作用，并且寻求组织领导的强力支持。有关我们对此重要主题的其他发现，请参阅 #安全成果# 博客系列。

“毫无疑问，新冠疫情危机会导致额外的安全威胁，因为员工需要更经常地在非常规情况下工作。我们主要必须做好三件事：为师生配备合适的教学工具、加强合理的安全措施，对教职员工进行威胁培训，并且不断强化他们对那些威胁的认识。参与很重要，正所谓“滴水穿石”，不断提供有效且合理的建议有助确保他们的家庭网络环境安全可靠。”

Mick Jenkins，伦敦布鲁内尔大学首席信息安全官

成功路线图

在本研究报告的前面部分，我们告诉那些希望了解主要成功因素之外更多信息的读者稍等片刻，我们之后会再回顾这个问题。现在，我们就要兑现承诺，好好探讨一番。图 15 底部显示了本报告中讨论的所有安全实践，左侧显示了所有计划级别的成果。有关实践和成果的完整问题文本，请参阅附录。

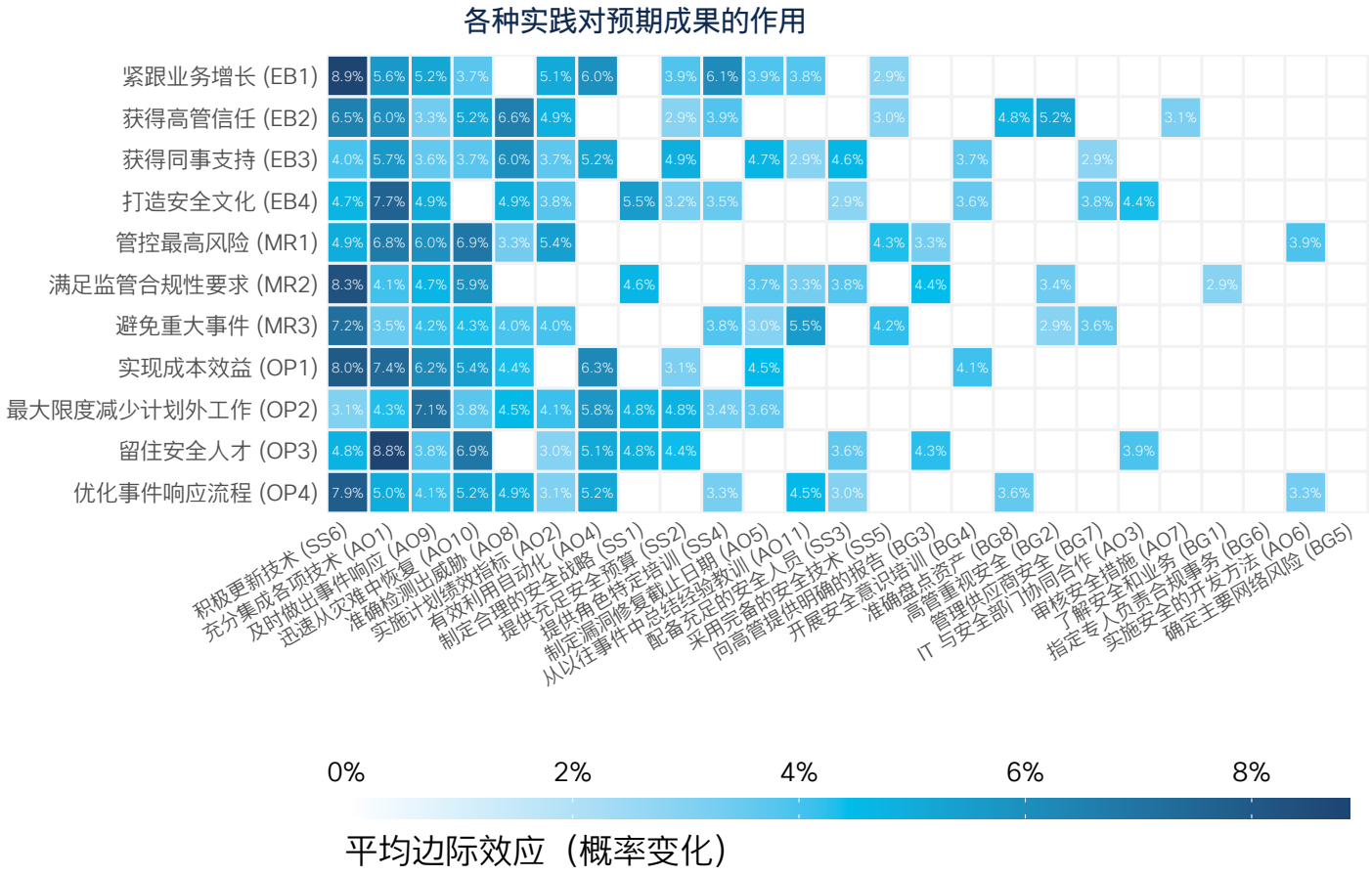
有色方框表示相交的实践和成果之间具有统计学上显著的正相关关系（白色方框表示无相关性）。方框阴影强度表示每个实践与成果的组合可以促进成功概率提升的幅度。阴影下的值对应于之前图表中所示的值。

我们认为，我们应该以与开头相同的方式来结束本报告，即让数据说话，而不是直接提供一堆建议。我们设计此图表的目的是帮助您直观地了解整体局势，并开始构建基于证据的路线图，以实现更成功的安全计划。最终，您需要自行选择自己的安全计划之旅。

在规划这一旅程时，请注意以下几项技巧：

- 如果想要确定根据相关数据，哪些实践有助于您的计划取得特定成果，请关注图中的各横行。
- 如果希望了解特定实践对于您的计划（成果）的潜在作用，请关注各个纵列。
- 请注意，有些实践对于很多成果都有广泛的影响，而有些实践只对特定成果具有有限的作用。

图 15：与各项安全计划成果相关的所有安全实践



来源：思科 2021 年安全成果研究报告

在图 15 中，空白方框不一定表示相应实践对实现各项成果毫无用处，这只是意味着，从全体受访者来看，平均而言，其影响不具有统计显著性。如果按行业、地区或组织规模对数据进行分段，结果会有显著变化。换句话说，您所处的阶段可能会有所不同。如果您对其中一些观点感兴趣，可以在地区报告和垂直行业报告中找到更多洞察信息，具体请访问 cisco.com/go/SecurityOutcomes。

感谢您抽出宝贵时间阅读此安全成果研究报告。安全行业报告不胜枚举，纷纷都在博取您的注意，我们希望此报告为您提供了一些基于数据的切实可行的洞察，以帮助您构建更成功的安全计划。如果在您追求这项崇高目标的过程中我们可以提供支持，请告知我们；此外，请在社交平台上使用 #安全成果# 标签参加我们的对话。

关于 Cisco Secure

思科长期以来一直是网络行业领导者，在此过程中构建了一个开放的集成式网络安全解决方案组合。我们认为，各项安全解决方案应该像一个团队一样协同合作。它们应该互相学习，作为一个统一整体去发现问题并作出响应。在这种情况下，安全系统性和效力才能得以提升。作为全球最大的 IT 基础设施和网络服务提供商以及全球最大的 B2B 网络安全企业，多年来我们一直深受客户的信赖。

Cisco Secure 秉持不断优化、简化的安全原则。我们提供以客户为中心的精简安全方法，可确保各产品不仅易于部署、易于管理、易于使用，而且可以协同工作。我们深知，客户及其相关人员是我们产品和服务的核心，他们希望消除复杂性和干扰，获得可靠的安全解决方案，注重最终成果。这就要求我们做到简化而不过于简单。我们的云原生平台在这方面实现了巨大飞跃。

利用 Cisco SecureX 平台，我们可以为安全行业提供可靠的安全解决方案，确保您在当下和未来免受威胁困扰。我们提供全球最全面、集成度最高的网络安全平台，帮助财富 100 强公司防御当前和未来的各种威胁。如需详细了解我们如何简化体验，促进您取得成功并提供面向未来的安全保护，请访问 cisco.com/go/secure。

美洲总部
思科系统公司
加州圣荷西

亚太地区总部
Cisco Systems (USA), Pte. Ltd.
新加坡

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

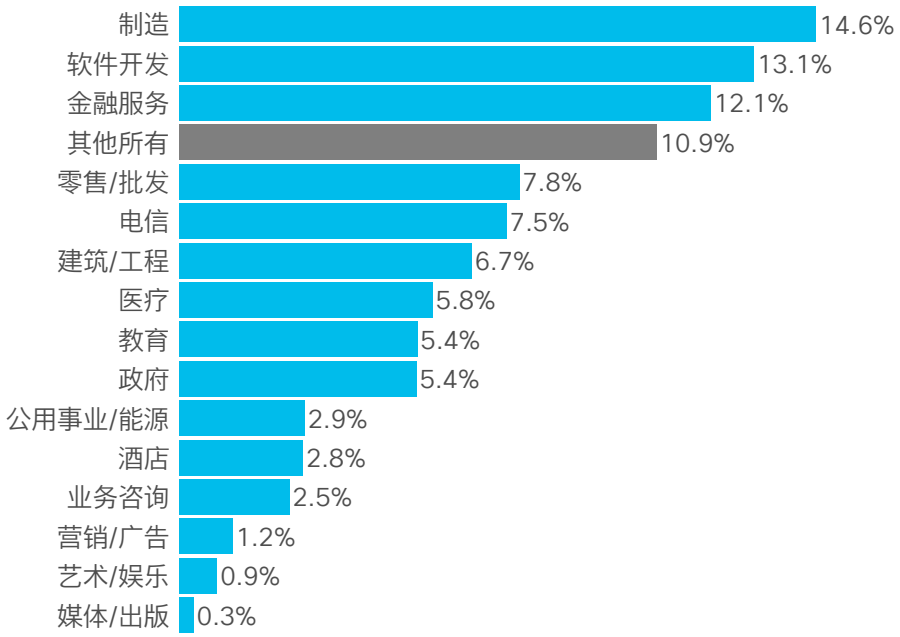
2020 年 12 越发布 RPT_12_2020

cisco SECURE

附页

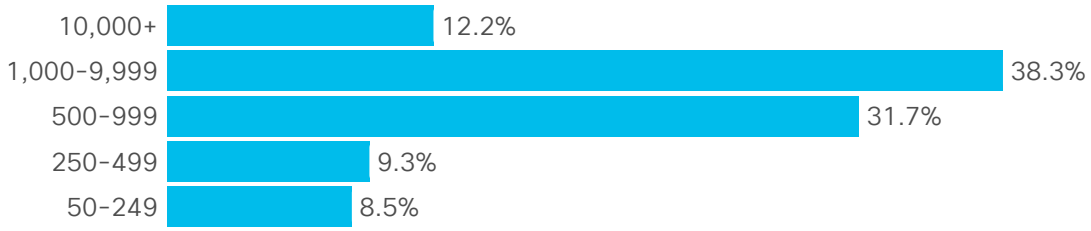
附录 A：抽样调查对象的背景特征

代表行业：



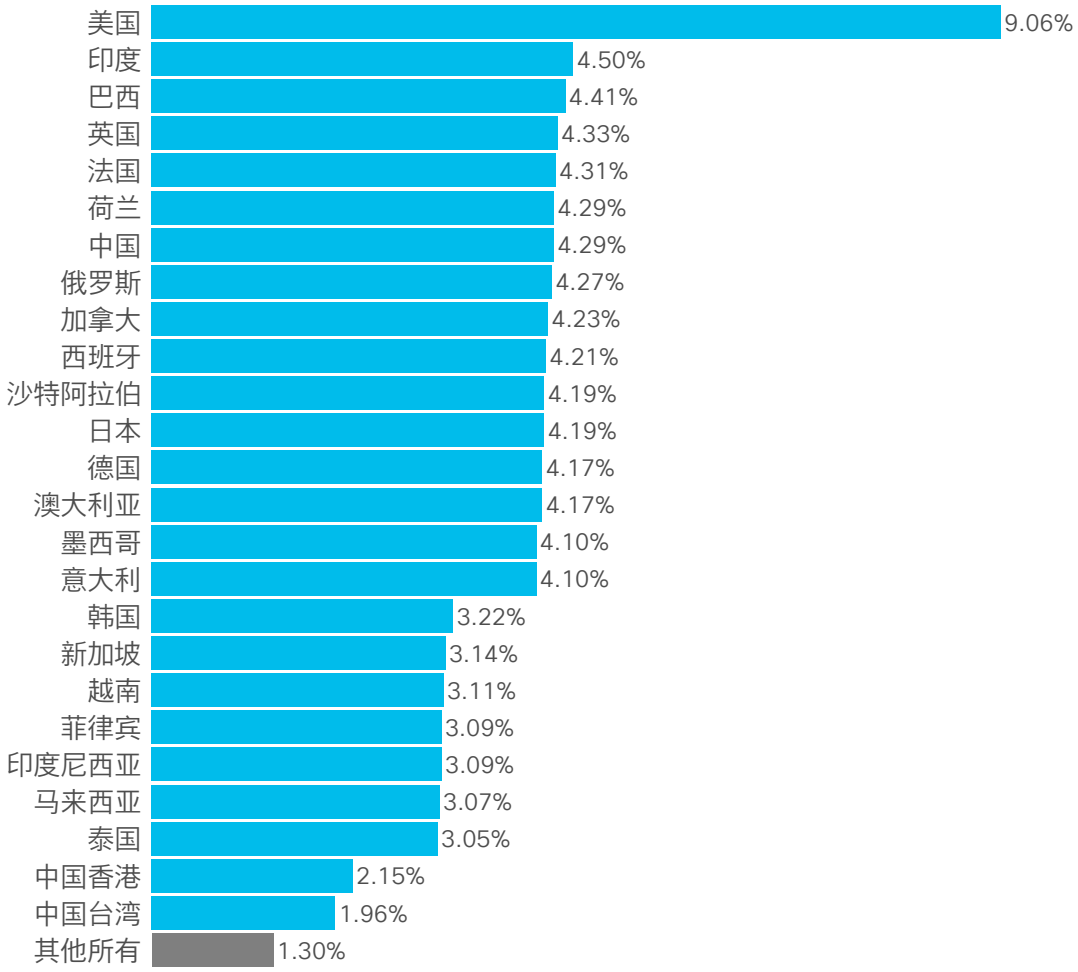
来源：思科 2021 年安全成果研究报告

代表公司规模（员工人数）：



来源：思科 2021 年安全成果研究报告

代表国家/地区：



来源：思科 2021 年安全成果研究报告

附录 B：完整的安全成果列表

推动业务发展	
EB1	**紧跟业务需求和业务增长**
	成功的示例和证据：安全计划能够充分应对不断变化的业务需求，而且不会阻碍新的收入来源。在某些情况下，安全解决方案可以提供竞争优势，甚至可以创造净收入。如果业务高管将安全部门视为单纯的成本中心或“无所作为的部门”，则表明组织在实现这一目标方面存在困难。
EB2	**获得高管领导层的信任**
	成功的示例和证据：安全主管定期与高层管理人员和董事会举行会议并获得支持。业务主管和安全主管之间保持一种相互尊重和协作的关系。如果安全计划频繁遭到高管质疑或合理要求经常得不到支持，则表明组织在实现这一目标方面存在困难。
EB3	**获得同事和其他组织单位的支持**
	成功的示例和证据：安全部门邀请其他部门参与协作，共同为组织构建安全防御。彼此密切沟通和协作，相互支持，共同实现更大的利益。非安全主管或部门也会制定与安全相关的绩效指标。如果部门间相互抱怨和争执，则表明组织在实现这一目标方面存在困难。
EB4	**打造全员支持的安全文化**
	成功的示例和证据：员工被视为安全解决方案的一部分，而不是问题所在。在员工满意度调查或离职会谈中，安全不是影响员工满意度或导致其离职的负面因素。非安全人员会定期报告其所发现的网络钓鱼尝试、潜在恶意软件和其他事件。如果频繁出现安全策略违规和权变措施，则表明组织在实现这一目标方面存在困难。
管控风险	
MR1	**管控组织面临的主要网络风险**
	成功的示例和证据：高管和安全主管就最常见的风险场景达成一致，并为应对这些风险制定了缓解计划（或相应安全计划获得了认可）。目前，潜在的网络风险处于领导层确定的风险偏好范围之内。没有迹象表明风险管控功能存在缺陷（例如，频繁出现未遂安全事件、控制偏差、响应/恢复测试失败等）。
MR2	**满足法规合规性要求**
	成功的示例和证据：审计人员和监管机构找不到安全方面本可以避免的隐患。组织一直努力跟踪和应对不断变化的法规要求。有证据表明，组织了解法规要求，及时确认发现的任何问题和不足，并通过加大投入/加强工作来缓解这些问题。
MR3	**避免重大安全事件和损失**
	成功的示例和证据：我们认为，在实现这一目标方面取得巨大成功的组织在过去几年中未发生重大安全事件（对内部和/或外部都具备较高可视性）。此外，我们没有理由认为，组织迟早会发生重大数据丢失事件。预计组织会出现轻微甚至中等程度的事件，但关键是组织是否已经并将继续保持杜绝重大安全事件。

实现高效运维	
OP1	实行具有成本效益的安全计划
	成功的示例和证据：高管认为安全计划实现了良好的投资回报 (ROI)。没有因为安全成本过高导致怨声载道。购买的产品闲置率较低。人员配备精简但够用。高管和安全主管共同制定了相应计划，可在不增加风险的情况下减少安全预算，这是一个良好的成功标志。
OP2	最大限度减少计划外工作和精力浪费
	成功的示例和证据：战略执行过程不会频繁出现挫折和偏差。安全预算属于主动支出而非被动应对。员工将时间用在更高级、更有价值的任务上，而不是陷入单调机械的工作，分身乏术。如果持续不断出现被动紧急救援或通过安全计划 “无法摆脱困境”，则表明组织在实现此目标方面存在困难。
OP3	吸引和留住安全专业人才
	成功的示例和证据：组织在安全行业享有良好的声誉，已经成为一个理想的工作单位。空缺的安全职位通常会得到快速填补，而无需提供额外的激励。人才不断晋升发展而不是纷纷离职，人才流失率较低。员工满意度一直很高。
OP4	优化事件检测和响应流程
	成功的示例和证据：安全运维被公认为卓有成效。安全事件的甄别有理有据，而不是基于猜测，而且无需耗费大量时间。对事件的响应和补救组织有序，而不是杂乱无章。组织会跟踪威胁检测时间和补救时间等指标，并且这些时间指标呈现不断下降的趋势。

附录 C：完整的安全实践列表

业务和治理	
BG1	我清楚地了解，我参与的安全计划可以如何支持我的组织实现业务需求和目标
BG2	我有充分的理由相信，我的组织的高管认为安全对于实现业务目标至关重要
BG3	我的组织的高管会收到有关安全计划的活动和成效的明确报告
BG4	我组织中的所有员工都会获得有效的安全意识培训，涉及威胁、策略和与其工作相关的规程等主题
BG5	我知道我的组织确定的主要网络风险，并且相信我们已经准确评估了这些风险
BG6	我的组织中有人负责管理安全和隐私合规性要求
BG7	我相信，我的组织价值链/供应链中的供应商的安全实践符合我们的标准，或者我们可以相应地进行管理
BG8	我的组织维护着关键系统和数据的准确资产清单，并根据安全要求和业务关键性对这些资产进行分类
战略和支出	
SS1	我们的安全计划秉持合理的整体战略，以成功实现其目标
SS2	我们的安全计划拥有成功实现其目标所需的财务预算
SS3	我们的安全计划拥有成功完成任务所需的人员
SS4	我们的安全人员接受成功履行职责所需的角色特定培训
SS5	我们的安全计划拥有成功实现其目标所需的技术和工具
SS6	我的组织制定了积极更新技术的战略，频繁升级采用最佳技术 IT 和安全技术
架构和运维	
AO1	我们的各种安全技术充分集成，可以有效地共同发挥作用
AO2	我们的安全计划使用性能指标来推动运维决策和行动
AO3	我的组织的 IT、开发和安全运维人员可以有效地协作
AO4	我们卓有成效地利用自动化技术来提高安全运维工作和人员的效率
AO5	我的组织遵守既定的服务级别协议 (SLA) 或补救系统和软件中暴露的漏洞的截止日期要求
AO6	我的组织采用严格的方法来开发和持续维护内部应用的安全
AO7	我们的安全措施受到积极监控和定期审查，以验证并保持其有效性
AO8	我们的威胁检测功能可以准确地感知潜在的安全事件，而不存在明显的盲点
AO9	我们的事件响应功能可对安全事件实现及时有效的调查和补救
AO10	我们的恢复功能可最大限度减少影响，并确保及时恢复受安全事件影响的资产
AO11	我们会特别努力从事件响应中吸取经验教训，并利用这些经验教训改进针对未来事件的安全措施

CISCO

SECURE

The bridge to possible