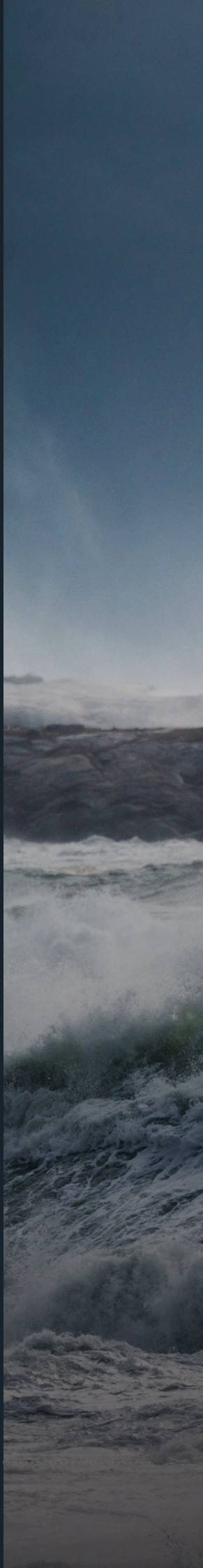
网络安全：如何战胜“最强风暴”？

《2021安永全球信息安全调查报告》

The better the question.
The better the answer.
The better the world works.

EY 安永
Building a better working world

目录



前言

《2021安永全球信息安全调查报告》发现，首席信息安全官与网络安全领导者正在对抗着由新冠肺炎疫情所引发的新一波威胁。

《2021安永全球信息安全调查报告》(以下简称“GISS调查报告”) **表明，在力争成为业务发展推动力和业务战略合作伙伴的道路上，疫情危机为网络安全职能部门带来巨大的挑战。**

我们调查了全球超过1,000位网络安全团队主管，发现首席信息安全官面临诸如预算不足、多头监管、跨职能沟通有待增强等问题。

的确，疫情全球大流行造成的最强风暴使得各种威胁肆虐。自2020年发布上一期调查报告以来，高破坏性且高复杂度的网络攻击数量有所增长，而如果公司已经将Security by Design应用于企业各个层面，则可避免很多攻击。

与以往相比，首席信息安全官与企业的关系也处在更严峻的压力之下，企业因此面临更大的网络风险。除此之外，预算限制意味着首席信息安全官需要努力缩小需求和资金之间的缺口。

在全球疫情好转之前，局势仍可能会进一步恶化。企业需要在后疫情时代加大技术和创新层面的投资，确保具有足够的韧性面对下一次大规模网络破坏。然而，很多企业尚未解决其在疫情最严重时期的转型所引入的延期风险和潜在漏洞。

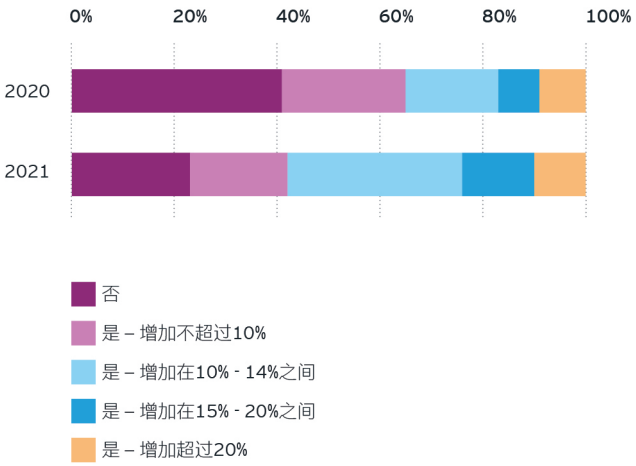
首席信息安全官正站在十字路口。为应对各种复杂而耗费精力的问题，他们必须迅速采取行动。我们的报告概述了网络安全领导者需要了解的当前工作环境以及他们需要采取什么行动来改变环境 。

1 首席信息安全官：站在十字路口

充满压力、变革和机遇的时代

图1

过去12个月内，您是否发现破坏性攻击数量有所增加?



在过去的一年里，每个企业都不得不适应某种形式的颠覆。锐意进取的企业快速推出了新的面向客户的技术和基于云技术的工具，以支持远程工作并保持市场渠道的开放，如此短的时间在不久前还被认为难以实现。

但是如此这般的变革速度也可能给企业带来沉重的代价。很多企业由于疏漏或行动紧迫性未将网络安全纳入决策流程，导致新的漏洞进入了快速变化的环境，并持续威胁当下的企业。

快速转型带来新的风险

在本调查报告撰写期间，首席信息安全官和他们的团队可能还没有完成关于公司所使用新技术对其防御体系所产生的长期影响的全面评估。与此同时，他们的同事仍在继续使用这些新技术。

“危机的紧迫性在于，即使企业开放了以前从未开放的系统，网络安全也仍然被忽视，”安永亚太区网络安全咨询业务主管合伙人Richard Watson表示，“不是所有企业都承认现在需要回过头来解决这些问题。”

然而，如果继续前进却不解决这类问题，将造成实实在在且日益紧迫的风险。在今年的GISS调查报告中，超过四分之三（77%）的受访者表示，过去12个月以来，破坏性网络攻击（如勒索软件）的数量与日俱增。与之相对应的，2020年只有59%的受访者表示此类攻击数量增加（参见图1）。

> “我专注于了解现有和未知威胁的影响，然后在产品开发过程中嵌入效率、安全及隐私设计。
>
> **Roland Cloutier**
> 字节跳动全球首席安全官

43% 的受访者表示他们十分担心自己管理网络威胁的能力。

但首席信息安全官很难扩大其影响力。大多数受访者（56%）承认，在管理层制定紧急战略决策时并不会咨询网络安全团队，或者咨询得太晚。虽然有受访者表示这种情况“不经常”发生，但只要发生一次，防御系统的缺陷就可能会被威胁者所利用（参见图2）。

这将导致对未来的焦虑。“我们努力使网络安全成为一种推动力量，”Richard Watson称，“但是仍然有企业在项目上线前夕才将其报告给网络安全部门。”

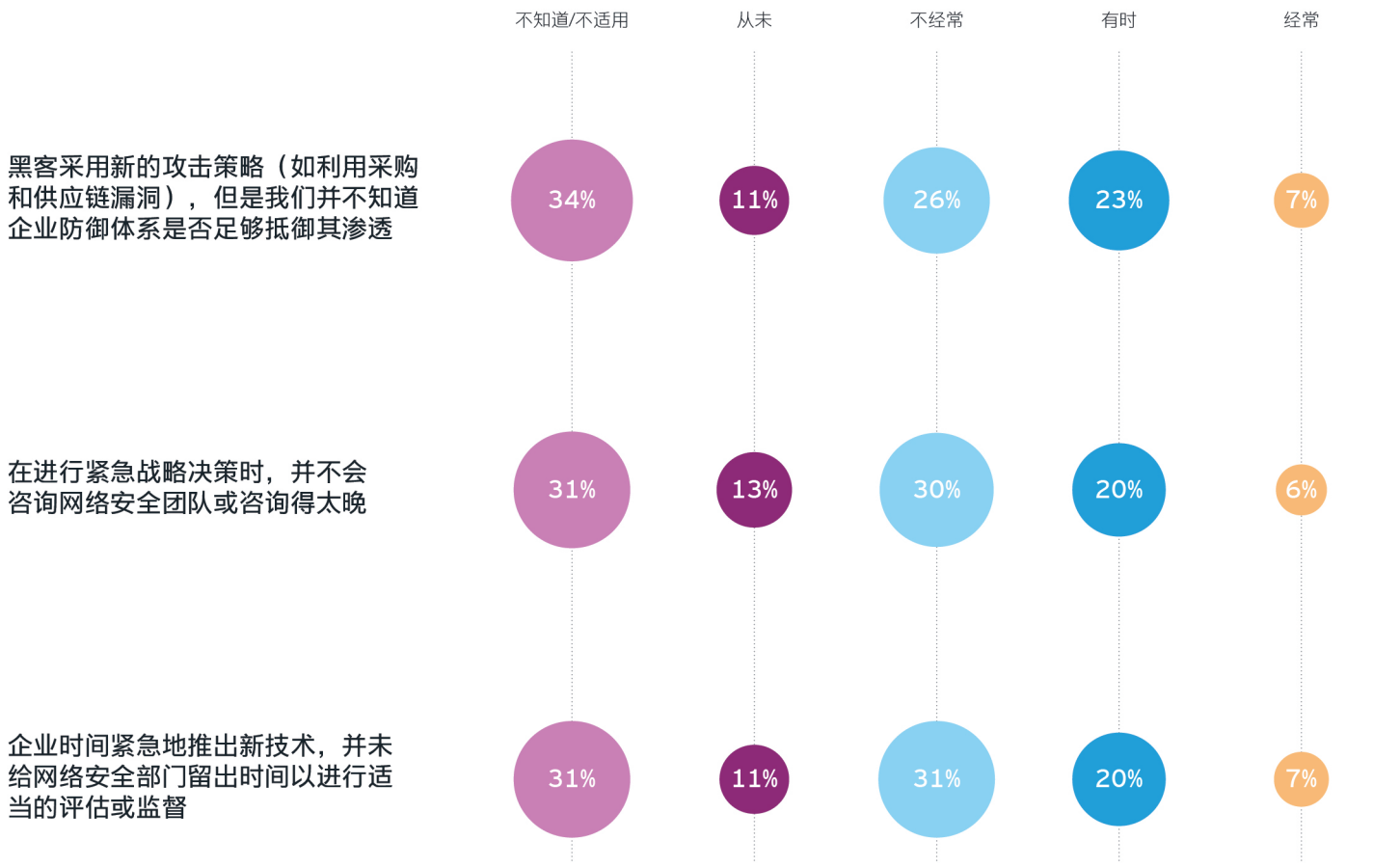
在最糟糕的情况下，首席信息安全官发现企业可能忽视其发出的警告。在本年度的GISS调查报告中，43%的受访者表示他们从未如此担心能否控制住网络威胁。而这种情况本是可以避免的。

字节跳动——快速部署，Security by Design

短视频及娱乐平台字节跳动的全球首席安全官（CSO）Roland Cloutier深度参与每周的战略决策。“内容可以是用户增长战略，也可以是新的盈利方式或音乐产品，”他称，“所有这一切都涉及新技术的建设和推广。我专注于了解现有和未知威胁的影响，然后在产品开发过程中嵌入速度、安全性以及隐私设计。然后，让公司为即将迎来的新资讯做好准备。我们如何以互联网发展的速度和文化传播的速度做到这一点？这就是这份工作的乐趣所在。”

图2

您的企业发生以下事件的频率为？



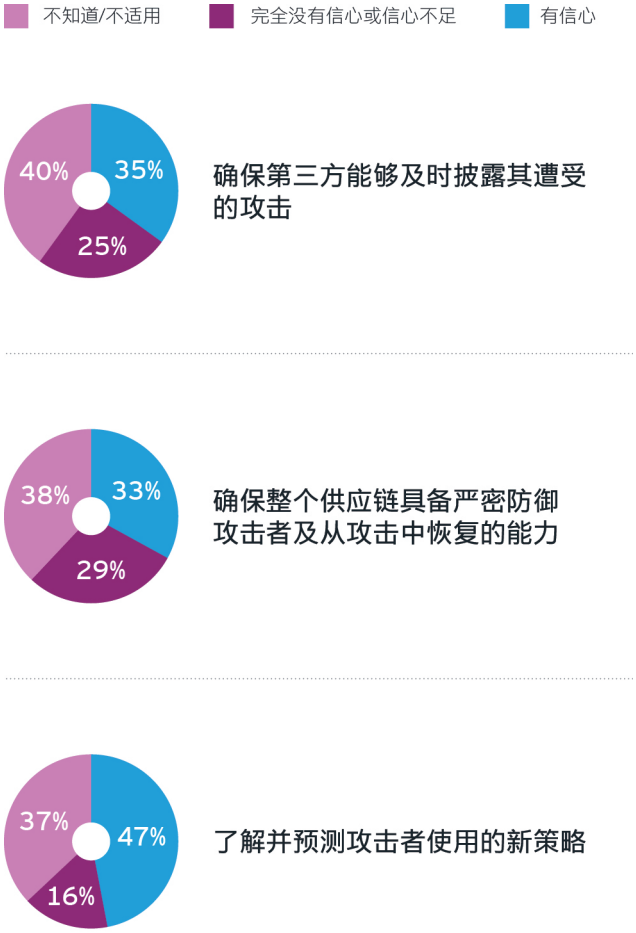
不到一半

47%

的受访者表示他们理解并能够预测攻击者使用的策略。

图3

对于团队在以下领域的能力，您有多大信心？



网络威胁格局日新月异，攻击手段层出不穷

在过去的一年里，无论是通过员工转发包含恶意软件的网络钓鱼活动还是通过利用客户购买的商业软件嵌入后门代码，威胁者正在不断地采用新策略来针对企业。

“现实情况就是，当下的威胁数量已远甚以往。”安永美洲区网络安全咨询业务主管合伙人Dave Burg表示，“这种现象的出现是受到勒索软件商业模式的推动，而事实也证明了这种模式非常有效。”

网络安全风险已升至峰值。2021年5月攻击并关闭了美国Colonial Pipeline公司的黑客便是通过暗网购买的“勒索软件即服务（ransomware as-a-service）”，这对整个经济和社会的重要组成部分构成了风险。与此同时，2020年攻击者通过大多数安全团队并不熟悉的复杂的供应链攻击渗透到SolarWinds达数月之久。

攻击者的目标越来越多，采用的攻击方式也愈加难以预测。只有三分之一的受访者表示有信心使供应链保持适当的稳固性或无懈可击（参见图3），这突显出了与采购和运营部门同事密切合作的重要性。仅有不到一半（47%）的受访者称其了解并能够预测攻击者使用的策略，例如，软件被攻击者渗透并出售给他们的客户从而导致安全事件。

这并不表示快速转型的需求已经消失。在本报告撰写期间，抗疫行动已经取得了重大进展，但企业要恢复“正常”仍需经历若干阶段。

根据《安永2021年首席执行官研究报告》

68% 的CEO计划在未来12个月内进行重大技术投资。

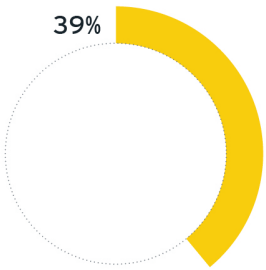
例如，雇主希望支持混合工作模式，同时在经济复苏中释放增长。安永最近的一项名为《重塑工作2021》（Work Reimagined 2021）的研究发现，54%的受访者在雇主拒绝其工作灵活性需求时会考虑辞职。首席信息安全官还应该意识到，一半的员工（48%）希望企业投资新的家庭办公技术，而企业若无法落实Security by Design，则可能面临更多的风险敞口。

首席信息安全官成为焦点

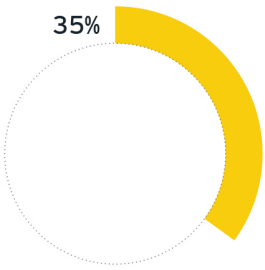
首席信息安全官正面临着一大关键时刻。根据《安永2021年首席执行官研究报告》（EY CEO Imperative Study 2021），68%的首席执行官正规划未来12个月内在数据和技术方面进行重大投资，如果首席信息安全官能够从规划阶段就支撑数字化转型，则将真正成为发展的战略推动者。而如果首席信息安全官无法在转型中发挥更加积极的作用，企业所面临的安全威胁则将进一步增加，同时他们在董事会的重要性也将降低。

图4

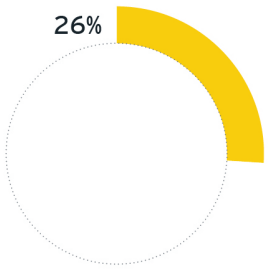
您的企业未来一年的计划中包含了以下哪些措施?



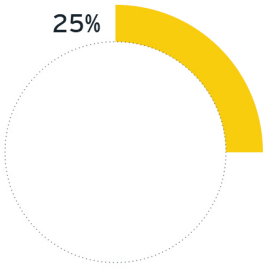
大规模投资数据和技术领域



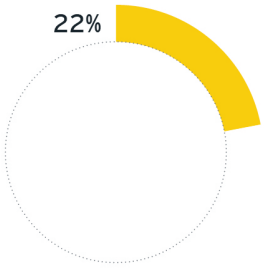
启动新的全面转型举措



大力降低成本



对产品或服务组合做出重大改变



员工人数大规模增长

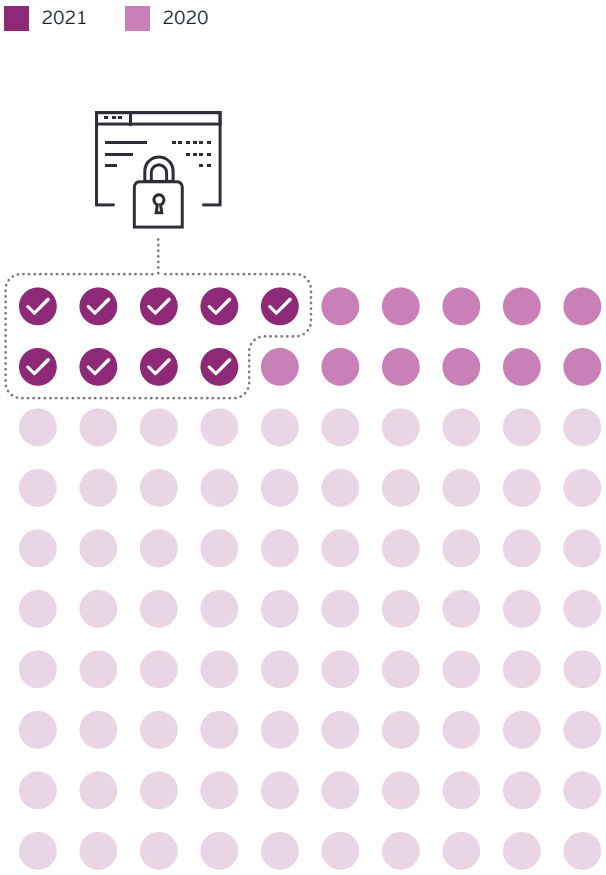
超过半数

55%

的受访者表示，如今网络安全受到的审查比他们职业生涯中的任何其他时期都要严格。

图5

仅有9%的董事会对其所在企业的网络安全风险缓解措施非常有信心——该数字与去年相比有所下降



高管层已经开始关注网络安全职能部门保护企业的能力。超过一半（55%）的受访者称，如今网络安全比他们职业生涯中的任何时候都更受到重视。十家企业中约有四家（39%）将网络安全列入季度董事会议程，相较于2020年的29%，这一比例有所上升。

于危机中育新机

若能够在降低风险的同时实现业务增长和技术发展，那么首席信息安全官将大有可为。大多数受访者（57%）认为这场危机为网络安全职能部门提供了增加关注度的机会。

Dave Burg积极督促首席信息安全官抓住这一机会以提高关注度。他表示：“我认识的很多首席信息安全官都被看作是明星，我们希望他们能够走到创新的前沿。”

那么，首席信息安全官是否已准备好抓住先机，成为新的发展推动者？能否在下一次大规模业务中断之前将韧性嵌入企业发展中？答案是肯定的，但前提是首先解决面临的三大关键的、相互关联的挑战：

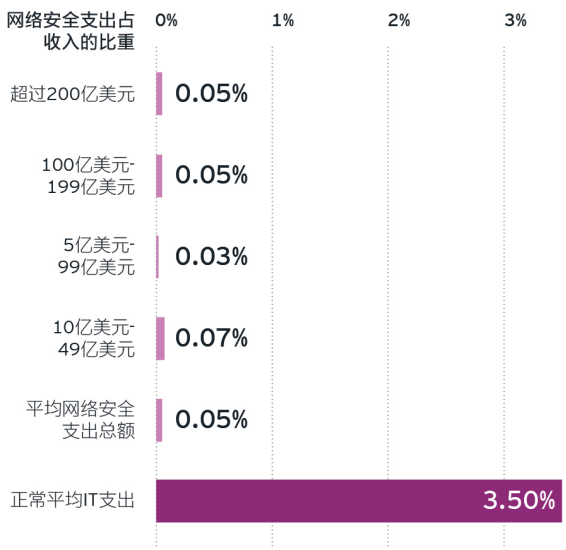
1. 网络安全部门的资金与需求仍存在较大差距，而此时较以往任何时候都更需要资金和资源的灵活支持；
2. “多头监管”为企业带来了更加严峻的合规挑战，需要更多的资源配置进行应对；
3. 网络安全部门与其他职能部门之间的关系仍有待改善，而此时是最需要建立更稳固关系的时候。

2 制约首席信息安全官行动的三大挑战

网络安全迎来最强风暴

图6

您的企业在网络安全方面的支出占年收入的比例是多少?



1. 当下的网络安全部门资金与需求仍存在较大差距

尽管网络攻击威胁日益严峻，但相对于整体信息技术支出，网络安全预算仍与需求存在较大差距。我们的调查数据还表明，即使需要敏捷应对疫情时代的波动性和未来被破坏的可能性，预算分配流程仍在很大程度上缺乏灵活性 。

“目前的融资模式根本不足以应对实际存在的风险，”安永全球网络安全咨询业务主管合伙人Kris Lovejoy表示，“这也表明，很多企业缺乏对网络问题的理解，未能建立基于Security by Design的企业文化。”

预算与需求不同步

在撰写本调查报告期间，安永对三位网络安全团队负责人进行了定性访谈，并调查了1,010位高级网络安全专业人士。受访企业去年平均收入约为110亿美元，而每年在网络安全方面的平均支出仅为528万美元，仅占收入的0.05%。

这种情况在不同行业之间也存在差异。举个极端的例子，在受到高度监管的金融服务与科技、媒体和电信（TMT）行业，受访者去年在网络安全领域的平均支出分别为943万美元和962万美元；而另一方面，能源公司的平均支出仅为217万美元。我们调查也发现不同规模的公司间也会存在差异，也有规模很小的公司支出比例很大。

我们的调查中，有一个问题涉及到预算的规划和分配。约有六成（61%）的受访者表示，网络安全预算是公司大项支出（如信息技术）的组成部分，19%的受访者表示该预算是固定的，并且会周期性地进行确认。超过三分之一（37%）的受访者表示，网络安全成本由整个企业分摊，但只有15%是动态分摊的，这取决于资源的使用情况。

换言之，很少有企业将其安全预算设定为经营所需的可变和或有成本。事实上，面对特定且快速发展的经营计划，首席信息安全官可能难以扩展其职能。

61% 的受访者表示网络安全预算是公司大项支出（如信息技术）的组成部分。

36% 的受访者认为他们遭受本可以通过投资避免的数据泄露事件只是时间问题。

成本削减产生新的脆弱性

首席信息安全官敏锐地意识到了企业因预算不足且不灵活而面临的脆弱性。

每10个受访者中就有4个（39%）表示，网络安全支出没有充分计入战略投资成本（如信息技术供应链转型）。超过三分之一（36%）的受访者表示，如果不在网络安全防御方面适当投资，企业遭受重大破坏只会是时间问题，而这本可以避免。

鉴于企业在面临业务中断的情况下急于寻求业务转型，可以预计，随着企业加大对发展的投资，网络安全预算不足这个问题将会加剧。39%的受访者表示其企业网络安全预算低于过去12个月应对新挑战所需的预算。

预算限制的一个不可避免的结果就是，首席信息安全官将需要做出艰难的决定：逐步减少本应在危机到来前就已启动的战略活动。超过一半（56%）预算不足的企业表示，他们不得不重新调整其网络安全要求。 44% 的受访者表示，他们不得不通过优化旧架构和旧系统以削减成本。

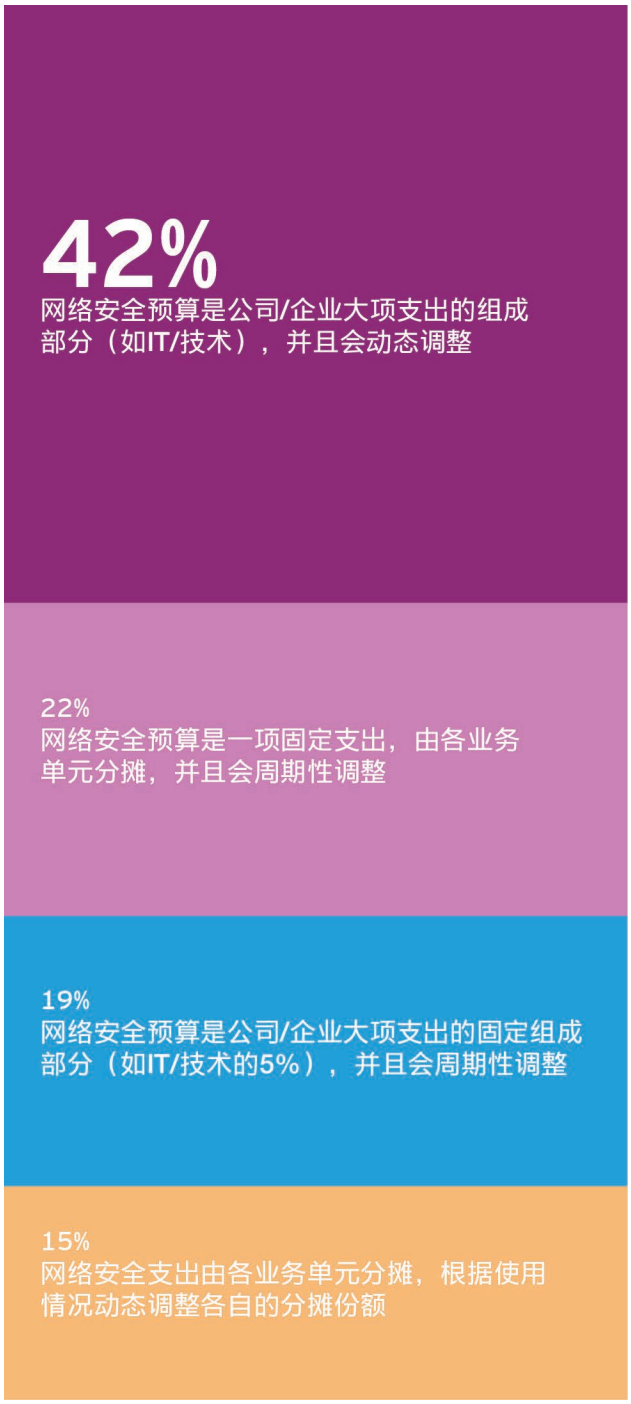
然而，少数企业确实对网络安全资金采取了更具战略性的方法。全球领先的保险公司Assicurazioni Generali集团首席安全官Remo Marini表示，Assicurazioni Generali公司采取了基于风险的方法为网络安全提供资金。“我们在安全、业务价值和降低风险这三方面的投资之间建立了直接关联，”他称，“我们的预算反映了复杂的规划活动，从对战略进行定义开始（通常为期三年），并收集所有内部和外部利益相关者提供的信息和意见。”

> “我们在安全投资、业务价值和降低风险这三方面之间建立了直接关联。

Remo Marini
Assicurazioni Generali集团首席安全官

图7

您如何确定企业的网络安全预算？

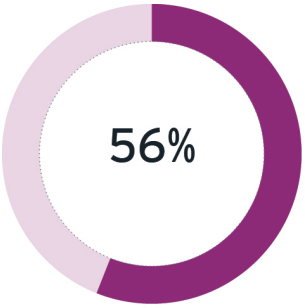


56%

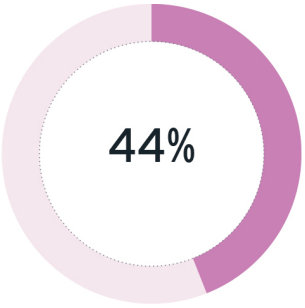
预算不足的受访者不得不重新调整其网络安全要求。

图8

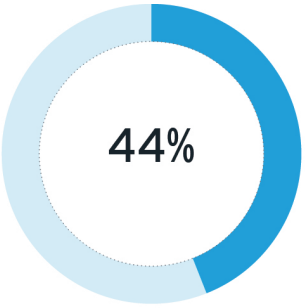
您采取了哪些措施以应对预算不足的情况?



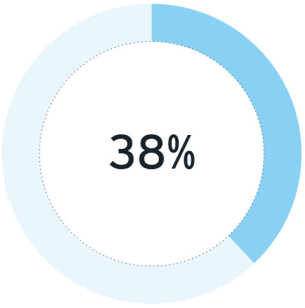
调整网络安全要求，以更好地满足不断变化的业务需求



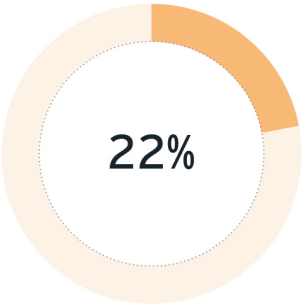
审视企业的传统架构，以寻求降低成本的机会



更加依赖第三方供应商



减少创新活动，专注于核心非战略任务



减少员工人数

2. “多头监管”为企业带来了更加严峻的合规挑战

全球合规环境正变得越来越复杂，各地管理体制分为区域和国家层面。某些行业（特别是金融服务业）企业还必须应对特定行业的监管。

安永欧洲、中东、印度及非洲区网络安全咨询业务主管合伙人Mike Maddison认为，监管问题正在变得愈加严峻。“如果贵企业是国际组织，那么应对这些互为重合又时有冲突的监管规定将极具挑战性，尤其在数据变得无所不在并且全球流动的情况下。”

监管合规需要企业投入更多的资源与时间

首席信息安全官为了满足监管合规要求，需要投入比以往更多的时间。一半（49%）的受访者称，确保合规可能是工作中压力最大的部分。约六成受访者（57%）预测，监管在未来几年将变得更加多样化。若首席信息安全官无法获取所需的资源，合规对其造成的压力是可想而知的。

“随着本地和国际监管机构的监管力度不断加大，监管议程正变得日益紧凑，”Assicurazioni Generali集团首席安全官Marini称，“法规数量的激增给企业带来了挑战，尤其是对国际化企业而言。标准化和通用的框架会更加有效率。”

另外需要关注的是，美国司法部已将勒索软件攻击提升到与恐怖主义同等的优先级，并正在通过华盛顿的一个工作小组协调调查 。在本报告撰写期间，尚不清楚该小组将会为遭遇网络攻击的私营企业提供哪些资源和帮助。

在预算层面，合规应当成为首席信息安全官的“朋友”

Kris Lovejoy认为，首席信息安全官对合规的看法发生了一些变化。“去年，首席信息安全官对合规的作用仍持有乐观态度，”她表示，“今年，他们认识到监管合规在过去一年的变化，其监管体系不断完善，监管制度愈加严格，监管要求日益细化，其复杂性为其带来了压力与担忧。”

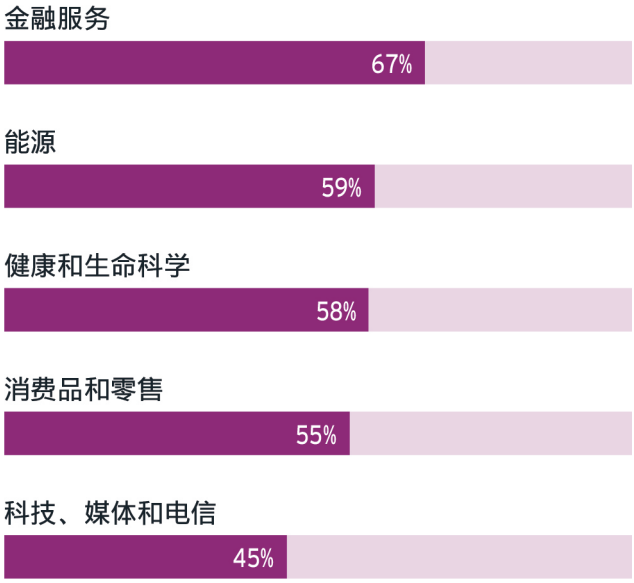
在Lovejoy看来，首席信息安全官应当将外部监管作为驱动力来促进企业改进网络安全体系。新的或者不断变化的合规监管要求，可能成为网络安全职能部门获取额外资金的途径之一，尤其是在预算紧张的情况下。

在今年的GISS调查报告中，35%的受访者认为合规有利于企业推动正确的关注重点与行动，与此同时，认为能够通过监管向董事会成功申请到额外预算的受访者不到五分之一（18%），这一比例略低于2020年（参见图10）。

当然，并非所有网络安全团队主管都对监管持悲观态度。TikTok的Roland Cloutier表示，监管至少占用了他50%或60%的时间，但总体上他仍保持积极态度。“我们的战略安全计划是基于监管因素和消费者保护的下一代要求，这是件好事。我们使产品能更好地面向未来，这有助于我们创建领先的行业概念，即如何成为一家致力于保护全球用户安全和隐私的企业。”

图9

您是否同意监管法规在未来几年将变得更加复杂化?

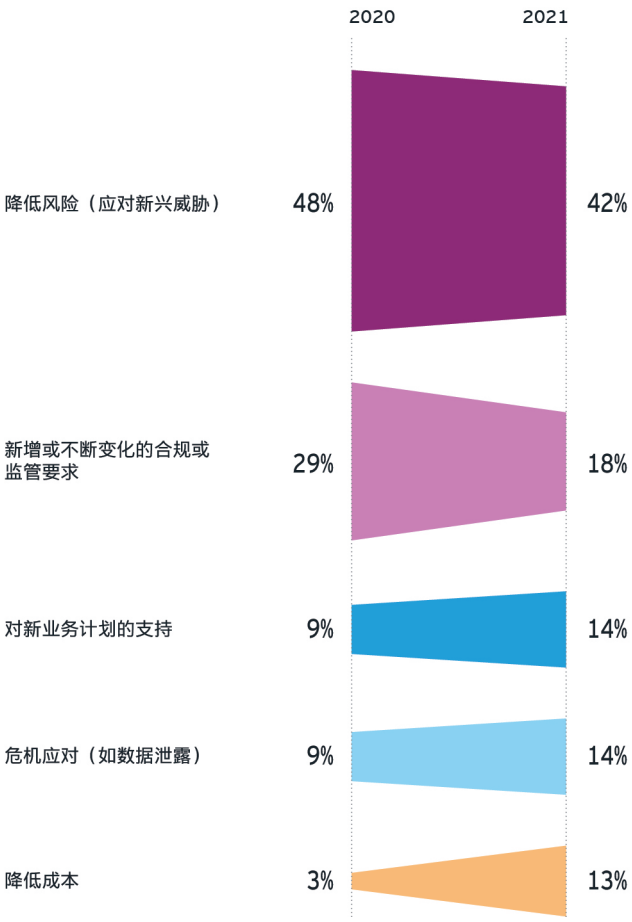


49% 的受访者表示确保合规可能是他们工作中压力最大的部分。

35% 的受访者认为合规推动了正确的行为。

图10

证明新增资金投入的合理性最简单的方法是什么？



> 疫情期间的动态环境对响应速度提出了极高的要求，因而有的企业可能会质疑网络安全团队是否拥有恰当的技能。

Mike Maddison
安永欧洲、中东、印度及非洲区网络安全咨询业务主管合伙人

3. 网络安全管理人员与其他职能之间的关系有待改善

为了管理战略转型带来的网络风险，首席信息安全官需要在投资决策的最初阶段提供咨询建议。但是，企业的网络安全部门和其他职能部门之间的关系缺乏积极性和稳定性，而这却对此类咨询至关重要。

首席信息安全官应与职能部门建立信任、共生的关系

长期以来，与业务高层的关系薄弱一直是首席信息安全官所担心的问题，而我们今年的GISS调查报告发现该问题依然存在。根据调查，网络安全经常缺席职能部门的重要对话。约六成（58%）受访者表示，他们的企业有时在实施新技术时并未留出足够的时间进行适当的网络安全评估或监督。

安永全球科技咨询业务主管合伙人Dan Higgins认为，首席信息安全官在新技术和数据解决方案部署流程中参与较晚，这令人担忧。他表示：“首席信息安全官必须在数字化转型的战略和解决方案架构阶段占据一席之地，才能主动地解决和规避掉这些风险。

这种趋势或许受到了企业高层的影响。根据《安永2021年首席执行官研究报告》，首席执行官已不再像2020年一样将网络安全列为其最关心的问题。他们在2021年的重点已转向采用新技术带来的挑战。

疫情大流行使情况变得更糟糕，81%的企业绕过了网络安全相关流程，并且在新业务的规划阶段未咨询网络安全团队。

“疫情期间的动态环境对速度提出了极高的要求，因而有的企业可能会质疑网络安全团队是否拥有恰当的技能，”Mike Maddison称，“企业文化是否正确？网络安全团队被视为阻碍力量还是提供有效解决方案的力量？如果企业对这些问题的回答存疑，企业其他部门就会在没有网络安全团队支持的情况下独自行动。”

在需要建立稳固关系的地方，关系却最为脆弱

这个问题在这样的职能部门最为严重：未来几个月将推出和扩展新的基于云计算的技术，因此他们极有可能存在遭到黑客部署的勒索软件攻击的巨大风险。

在今年的研究中，41%的受访者认为他们与市场营销职能部门的关系亟需进一步改善与巩固，相较于去年的36%，这一比例有所提高。同时，28%的受访者表示他们与业务方的关系差强人意，而去年这一比例为23%。

调查结果表明，尽管在2020年有超过三分之一的受访者（36%）有信心在新业务的规划阶段咨询网络安全团队，但该数字在2021年已降至19%。

“网络安全部门与业务线、产品开发和市场营销部门的关系是消极的，而与风险、法律和信息技术部门的互动却是积极的，”Kris Lovejoy表示，“本质上，离你所在的规划周期越远，关系就会越积极，这就是问题所在。在最需要网络安全部门参与以支持增长的领域，却被相关方排除在外。”

41%

的受访者将他们与市场营销职能部门的关系描述为亟需进一步改善与巩固。

跨职能间的沟通应不断增强

团队之间沟通不畅导致很难求取进步。首席信息安全官称其很难让员工用业务术语表达出他们对网络安全咨询的需求。此外，业务方可能认识到了网络安全的传统优势（如控制风险），但并不总是将网络安全视为战略合作伙伴。

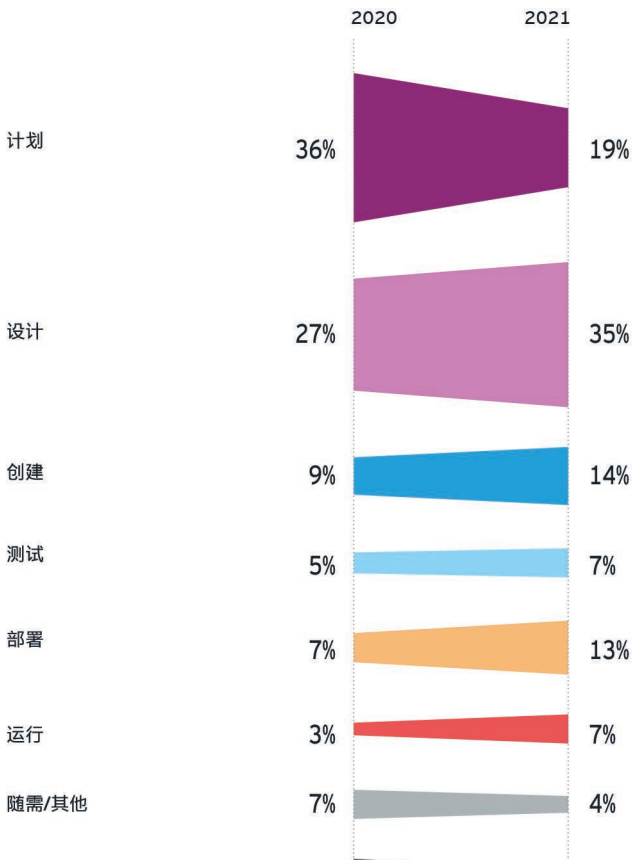
澳大利亚宽带网络公司 （NBN Co）首席安全官Darren Kane，参加了本报告的定性采访，但并未参与调查。他表示：“我已经发现各行业的心态都在积极转变，董事会认识到网络安全是一种风险。”“在打破沟通壁垒方面，首席信息安全官们仍有很多工作要做，例如他们要用不那么技术性的语言来沟通和表达，让董事会更好地了解潜在的业务风险。”

不到一半的受访者（44%）相信其团队能够与同事有共同语言，仅有26%的受访者认为高管层会使用同样的术语来描述网络安全职能部门。只有四分之一的受访者（25%）认为高级业务领导层会将网络安全职能部门描述为具有商业意识。

受访者承认，企业其他部门更有可能使用“保护业务”和“快速应对危机”来描述网络安全职能部门。虽然这些特质本身令人钦佩，但它们仍需要与沟通力、说服力和建立信任的能力相平衡。

图11

在哪一阶段将网络安全纳入到新的业务计划?

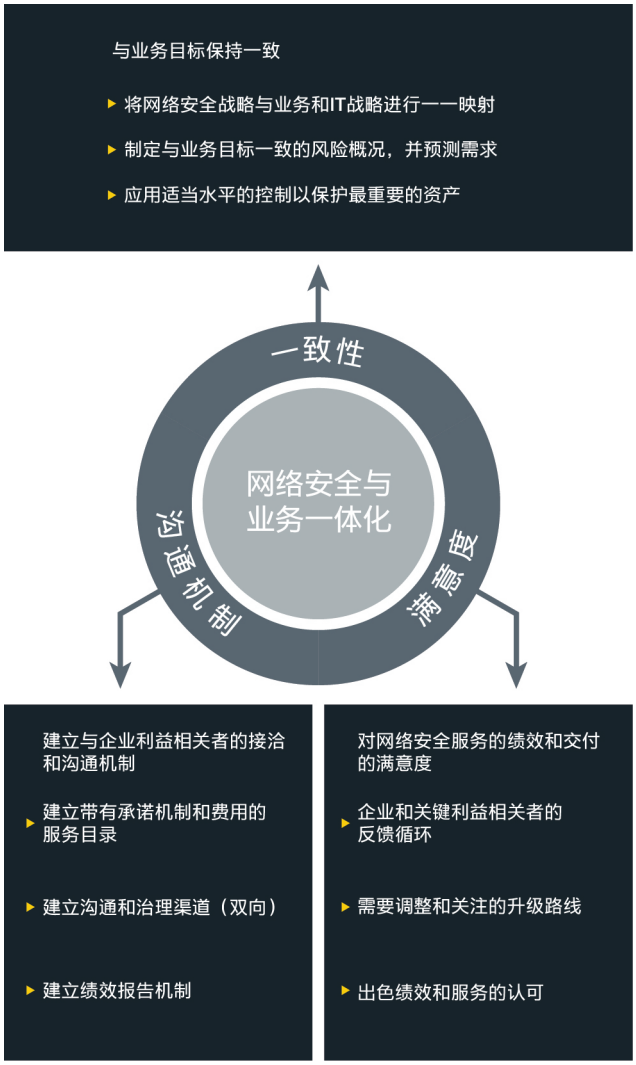


3 调查结论与下一步

首席信息安全官应作为价值推动的因素

> **首席信息安全官对企业转型和交付长期价值极为重要。**
>
> Errol Gardner
> 安永全球咨询服务副主席

图12



首席信息安全官如何应对本年度GISS调查报告所述的核心挑战？答案是，他们应该在企业中扮演更具战略性和商业意义的角色——将团队重塑为转型推动者，这一点毋庸置疑。

“首席信息安全官对企业转型和交付长期价值极为重要，”安永全球咨询服务副主席Errol Gardner表示。在讨论首席信息安全官应该如何将自己定位为转型推动者时，Gardner补充道:“虽然首席执行官正在实现他们的愿景，并通过技术成功实现企业转型，但不能对由此带来的网络风险视而不见。”

“与此同时，首席信息安全官有责任确保首席执行官恰当地了解投资网络安全所带来的价值，并认识到这是转型之旅不可或缺的一部分。建立首席信息安全官、首席执行官和其他的高级管理层人员之间的战略关系，将不仅有助于确保转型计划的成功，还可以确保其为企业及其人员采取了一种满足网络安全的方式。”但网络安全部门的管理层能否施加影响，并确保其他广泛业务能够支持其日益重要的角色，仍不得而知。根据《2021年安永全球董事会风险研究》的描述，80%的董事会认为改进风险管理对保护和创造价值至关重要，但我们认为首席信息安全官的贡献目前还未得到广泛认可。

我们的调查结果表明，建议首席信息安全官考虑3大核心措施，以提高其在企业中的地位:

- 重新评估他们与业务的一致性
- 审视人才画像
- 重点关注4个关键利益相关者群体

值得注意的是，除了相关思考过程中的一些变化，这些措施与2020年报告所给出的指导是一致的。而在危机时代爆发的种种事件进一步凸显了这些措施的紧迫性以及实施的恰当性。

> 没有“标准的”网络安全人才画像。

1

把握“最真实的情况”——重新评估您与业务的一致性

一直以来，网络安全团队在评估自身能力、识别风险和制定未来路线图方面都展现出极大的优势。

首席信息安全官应将注意力更多地集中于过去一直较为薄弱的网络安全要素上。具体而言，他们应该加强与利益相关者的合作，确保与核心业务目标保持一致，并评估其业务合作伙伴对安全服务的性能和交付的满意度（参见图12）。

近年来，由于首席信息安全官与业务合作伙伴的关系仍有待改善，首席信息安全官现在可能缺乏与其他职能部门同步运作以及推进符合企业发展的战略所需的可见性。

2

审视您的人才画像，但切勿不切实际

为了应对本调查报告指出的企业面临的挑战，以及网络攻击的复杂性，首席信息安全官需要全能复合型专业人士的支持。

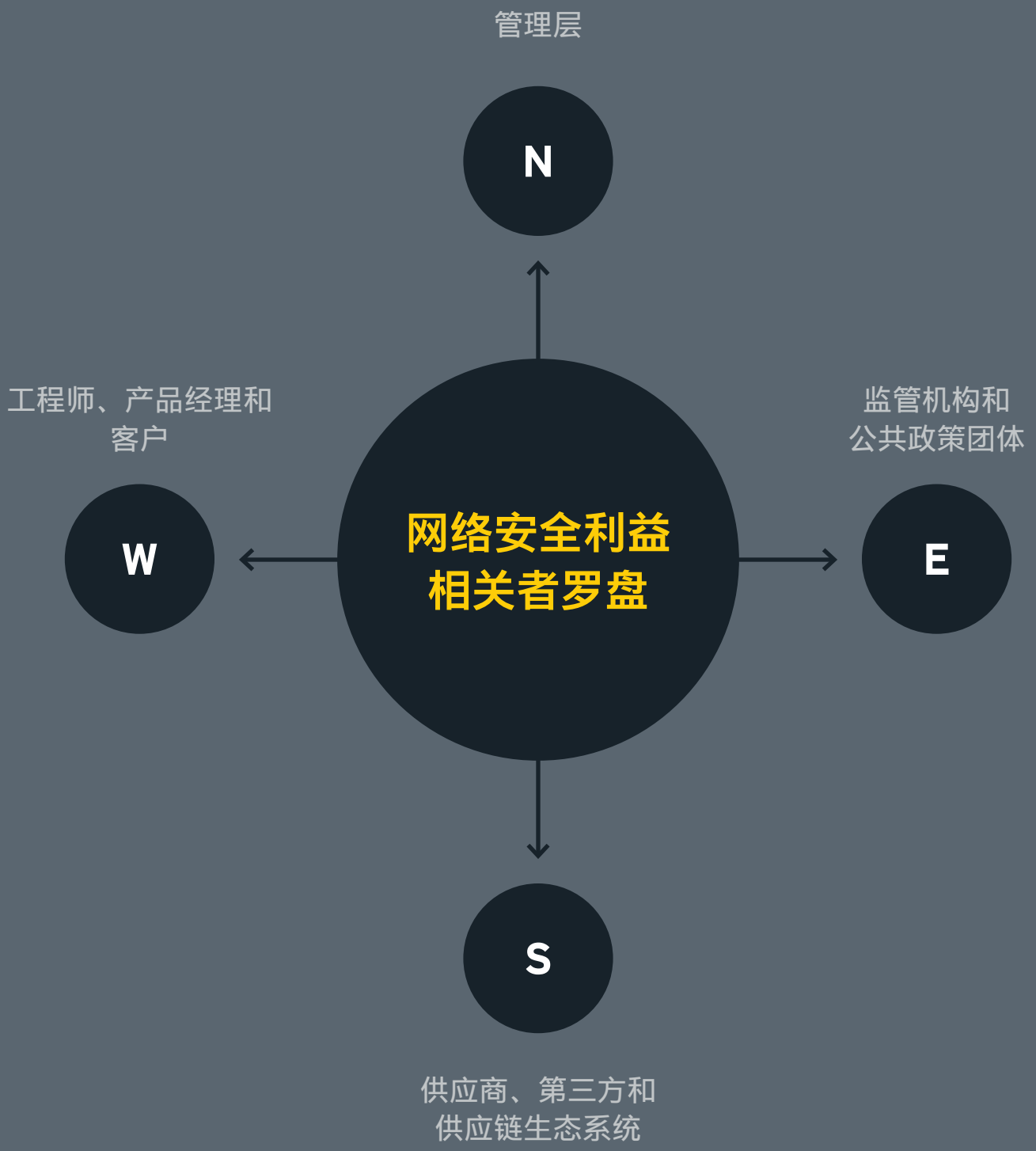
但当下网络安全职能所需的技能广度正在向几个方向同时扩展，这导致一个问题，即没有所谓“标准”的网络安全画像。首席信息安全官所需的人才要有先进的技术技能，以及拥有能够建立跨部门协作的能力。他们还要招揽追求创新和发展的人才，并能够发现新兴威胁和防御系统的漏洞和缺陷。

在图13中，我们列出了近年来出现的很多网络安全高管的画像。

图13: 当今网络安全职能部门中的多类型人才画像

网络安全管理人员概况	专注领域	优势	劣势
安全专家	所有与网络安全相关的	深厚的专业知识	缺少商业知识
技术支持人士	技术解决方案和工具	技术导向	孤岛式思维
风险和合规专业人士	风险、控制和合规	有益于受到高度监管的行业	缺少技术知识
业务转型者	业务整合	业务互联	缺少技术和安全知识
兼职人员和分工人员	网络安全及其他主要职责	节约成本	博而不精

图14: 首席信息安全官处于四个利益相关群体的中心



（虽然这一职业相对较新）。每个画像都有自己的关注领域，依靠自己的软技能和专业资格，并在满足不断变化的业务需求方面发挥重要作用。

然而，试图要招聘到拥有所有这些才能的人，实属不切实际。更优的方法是在理解每个学科都有自身优劣势的基础上，建立一个各学科百花齐放的团队。

在建立跨职能协作关系方面，首席信息安全官需要确保其团队成员能够更多地接触市场营销、创新和其他相关业务单元等职能部门。“网络技术人员以占据办公楼的地下室而闻名，”Darren Kane称，“但由于网络风险成为了所有企业的最高运营风险之一，网络团队应该更多地走出来并接触企业的其他部门。”

<< 首席信息安全官熟悉“左移”原则，力求在转型和产品开发生命周期的早期阶段将网络安全纳入其中。

3

日新月异——采取新的利益相关者罗盘

首席信息安全官都悉知“左移”（Shift Left）原则，设法在转型和产品开发生命周期的初期就嵌入网络安全。

然而，新冠肺炎疫情危机表明，左移不再是唯一需要的手段。我们建议首席信息安全官向北、向东、向南和向西移动。在实践中，这意味着他们需要引导四个关键利益相关者群体（如图14所示）。

处理“北边”的管理层所担心的问题，需要侧重报告和问责制，以及预算和资源分配问题。向“东边”的监管机构移动，则需侧重认证、鉴证以及监管要求映射。向“南边”移动，则需提高标准和增强测试。向“西边”移动，需要注重“Security by Design”“Privacy by Design”，与认证和持续测试。

如果首席信息安全官能够将自己置于这四个关键利益相关者的中心位置，则能够有效地提升职能的战略影响力。

风暴之外

新冠肺炎疫情给首席信息安全官敲响了警钟。企业希望网络安全团队能够保护其免受不断变化的网络威胁，同时加快推进技术转型和业务增长。

毫无疑问，很多首席信息安全官已经迎接了挑战，并且可以证明其角色不断提升的战略重要性。但公平地说，这场危机还显现出了网络安全的弱点和需要改进的领域。具体而言，首席信息安全官仍需要再接再厉，在与最高管理层建立更为牢固的、基于信任的关系的同时，应用好“Security by Design”。

这并非轻而易举就可达成，也无法在一年内就实现，但企业对它的关注从未停止。首席信息安全官需要参与战略投资的规划，并且有责任争取在讨论桌上拥有一席之地。

联系我们

王海瑛
主管合伙人
大中华区咨询服务
安永（中国）企业咨询有限公司
+86 21 2228 3089
helen-hy.wang@cn.ey.com

梁尚文
主管合伙人
大中华区金融服务咨询
安永（中国）企业咨询有限公司
+86 10 58153236
sherman.leung@cn.ey.com

高轶峰
主管合伙人
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
+86 21 2228 6611
kelvin.gao@cn.ey.com

彭瑞明
合伙人
香港金融服务科技咨询
安永咨询服务有限公司
+852 2846 9085
jeremy.pizzala@hk.ey.com

兰瑜
合伙人
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
+86 10 5815 3951
bruce.lan@cn.ey.com

阮祺康
主管合伙人
中国金融服务科技咨询
安永（中国）企业咨询有限公司
+86 21 2228 7887
keith.yuen@cn.ey.com

施建俊
合伙人
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
+86 21 2228 7599
alex.shi@cn.ey.com

冯哲
合伙人
中国金融服务网络安全与隐私保护咨询
安永（中国）企业咨询有限公司
+86 21 2228 6855
wilson.z.feng@cn.ey.com

夏文婷
合伙人
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
+86 21 2228 3320
wendy.xia@cn.ey.com

胡立基
合伙人
大中华区网络安全与隐私保护咨询服务
安永（中国）企业咨询有限公司
+86 20 2881 2731
winson.woo@cn.ey.com

安永 | 建设更美好的商业世界

安永的宗旨是建设更美好的商业世界。我们致力帮助客户、员工及社会各界创造长期价值，同时在资本市场建立信任。

在数据及科技赋能下，安永的多元化团队通过鉴证服务，于150多个国家及地区构建信任，并协助企业成长、转型和运营。

在审计、咨询、法律、战略、税务与交易的专业服务领域，安永团队对当前最复杂迫切的挑战，提出更好的问题，从而发掘创新的解决方案。

APAC no. 03013167
ED None

ey.com/china

关于本调查报告

今年的GISS调查报告，其数据来源于2021年3月至5月对1,010家企业的首席信息安全官和其他高层领导展开的调查。首席信息安全官和其他高级管理层人员占受访者的50%；其他人员则是高级网络安全专业人士。调查主要通过电话进行，少数调查在网上完成。

GISS作为一项全球调查报告，其43%的受访者来自欧洲、中东、印度和非洲区，36%来自美洲区， 20%来自亚太区。受访者包括来自金融服务、消费品和零售、健康和生命科学、能源、政府和公营机构、科技、媒体和电信领域的首席信息安全官或与其相当的职能人员。本报告数据中包含的每个企业的年收入均超过10亿美元。

我们基于类似的同比样本数据，通过比较2020年的调查报告得到了 2020-2021年的实时快照。2020年的报告包含年收入低于10亿美元的企业，2021年的报告则不再包含该类企业。除该量化研究外，安永还在2021年4至6月与网络安全行业思想领袖展开了一系列深度讨论。