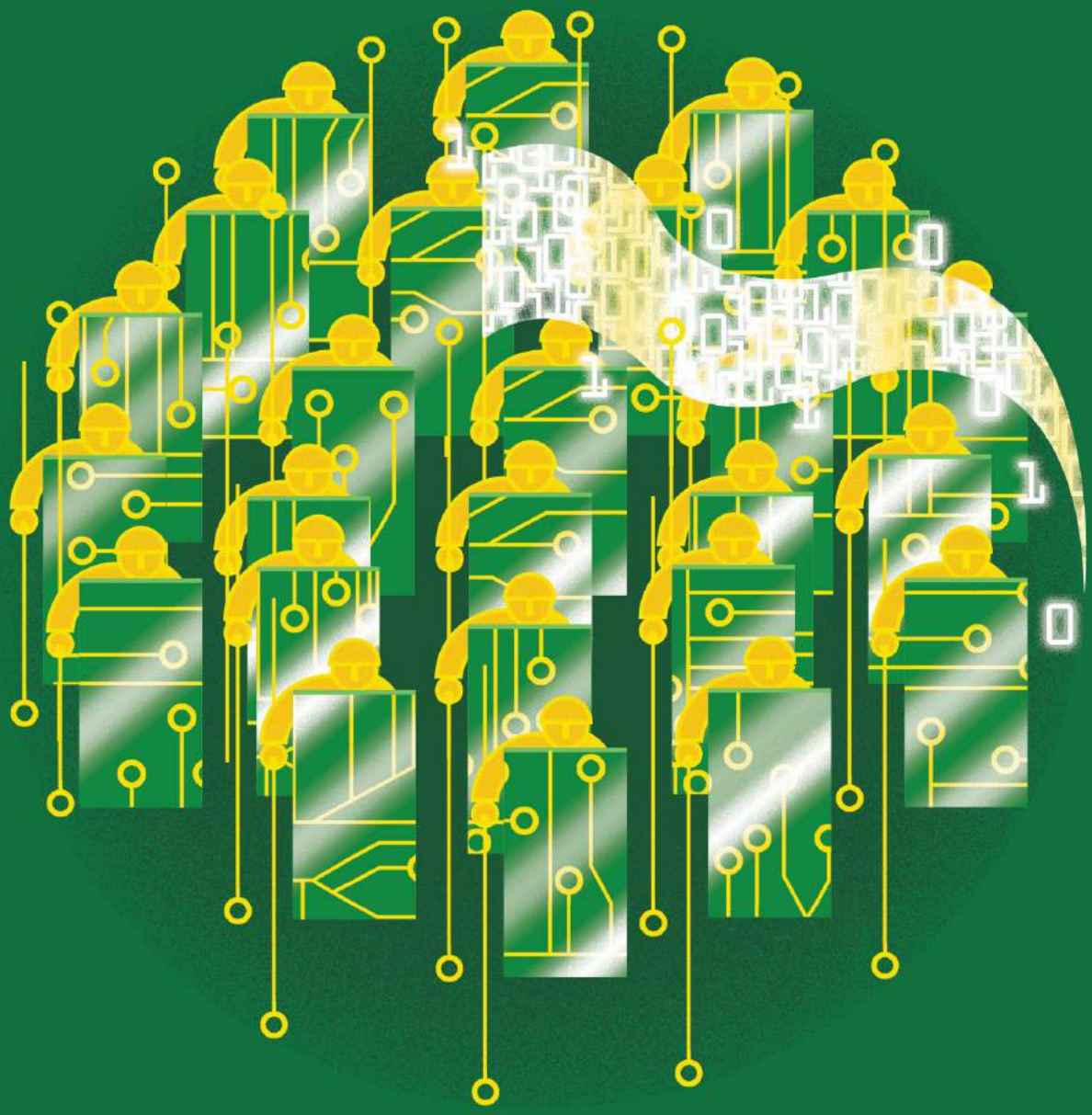
Deloitte.
Insights

FINANCIAL SERVICES | Information Sharing and Analysis Center



提升金融机构网络安全成熟度

风险管理领先实践

金融服务信息共享与分析中心(FS-ISAC) / 德勤网络风险服务首席信息安全官（CISO）年度调研与分析报告（第二期）

本报告由德勤金融服务行业研究中心及金融服务信息共享与分析中心（FS-ISAC）共同发布

德勤网络安全服务（Deloitte Cyber）助力企业构建自内而外的网络安全意识，帮助企业在面对持续变化的网络威胁时变得更强大、反应更敏捷，自身更具创新性，灵活应对挑战。

目录

关于本调研

本调研由金融服务信息共享和分析中心（FS-ISAC）与德勤网络风险服务共同完成。FS-ISAC是一家总部位于美国的行业联盟，成员包括近7,000家金融机构，致力于降低全球金融体系中的网络风险。本次调研共有97家企业参与，覆盖了不同规模企业（图1）和所有金融子行业（因部分受访企业可分属多个子行业，故图2数量总和超过97）。

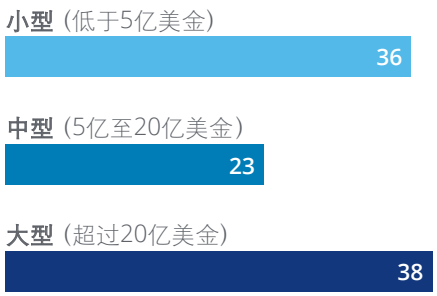
本调研考察了金融机构网络安全运营的多个环节，包括组织和管理网络安全活动，首席信息安全官（CISO）的汇报路线，董事会对CISO工作的关注程度，以及在财务方面应优先考虑哪些网络安全领域等。

调研还要求受访者提供其在国家标准与技术研究院（NIST）四级网络安全框架下的成熟度水平[1]（图3）。百分之八十的受访企业自行评估了他们的成熟度水平，其余则由第三方评估得出。在97家参与调查的企业中，74家反馈了对16个NIST网络安全框架下各不同控制项的单独评价。

根据每个控制项中成熟度的评分，17家企业被认定为成熟度达到自适应级，43家达到可重复级，12家达到可知晓级，剩下的两家为初始级。我们将网络安全成熟度判定为初始级的企业与可知晓级企业进行了分组合并，以确保本报告分析的严谨性。

图1

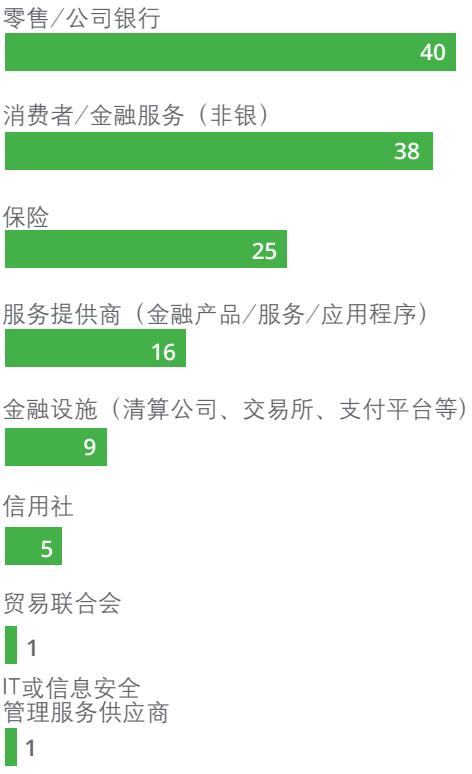
受访企业规模



注意：所有金额均以美元计算

图2

受访企业所处行业



资料来源：2019年FS-ISAC/德勤网络风险服务CISO调查，德勤金融服务行业研究中心。

引言

如今，数字化与物理技术的连接更加紧密。如何理解并识别网络风险的发生对金融机构至关重要。与此同时，网络安全团队必须不断努力履行其义务及监督职责，同时满足客户对隐私和创新业务解决方案不断提高的期望。

在过去的两年中，德勤与FS-ISAC进行合作，通过对FS-ISAC各成员单位就如何应对网络安全挑战进行调研，旨在评估各家网络安全预算和整体网络风险管理是否达到了良好状态。

在2018年的抽样调研中，我们了解了受访企业的CISO如何履行其职能和职责，进而对整个行业的网络安全战略、架构以及预算优先级提出了初步的见解。[2]

今年，除了根据行业、公司规模和网络风险管理成熟度来确定整个行业的预算支出模式外，我们还识别出那些已经达到NIST所定义的最高成熟度水平公司的几个核心特征 （参见图3）。

NIST网络安全成熟度框架[3]中所定义的“自适应级”的公司具备以下特征:

- 确保企业包括董事会及高级管理层的参与;
- 提升网络安全在企业内的重要程度。网络安全可以在信息技术（IT）部门外获得更高级别的关注和更强的影响力;
- 对网络安全的投入与公司业务战略保持紧密的协同一致。

图3

网络安全成熟度水平

初始级	企业没有正式的网络安全风险管理，风险管理多数是无序的、甚至是被动的。
可知晓级	风险管理实践由管理层批准，但没有在整个组织中形成政策。
可重复级	企业的风险管理活动获得管理层的批准，并形成政策与制度。
自适应级	企业根据网络安全活动中获取的经验教训和预测指标，自动调整其网络安全活动。

来源：国家标准与技术研究院（NIST），“提升关键基础设施安全框架”，2018年4月16日。

能够整合这些基本特征，并以网络安全行业领先实践为参考的组织，将更有可能适应不断变化的业务模式和应对来自日益白热化的外部竞争格局的威胁。

调查显示，单靠资金的投入可能无法解决网络安全问题，高昂的网络安全支出并不意味着能转化成更高的安全成熟水平。金融机构采用何种方式以更好的保护其数字资产安全，至少应与投入在网络安全方面的资金数量同样重要。

聚焦成本

了解企业对网络风险资源的投入是我们希望调研的重要信息之一（图4）。基于调研回复统计，企业将IT预算的6%到14%用于网络安全，平均用于网络安全费用为IT总预算的10%；相比企业总收入，这一数字约为0.2%到0.9%，平均约为0.3%；若分析人均网络安全支出，受访者为每位全职或同等员工支付1,300至3,000美元，平均则2,300美元。

不同规模的企业在网络安全领域的支出差异明显（图5）。显而易见的是，规模较小的企业需要加快脚步，才能赶上规模较大企业对网络安全的投入。接受调查的小型企业在网络安全方面的支出占其收入的比例(0.2%)，几乎仅为中型企业(0.5%)或大型企业(0.4%)的一半。

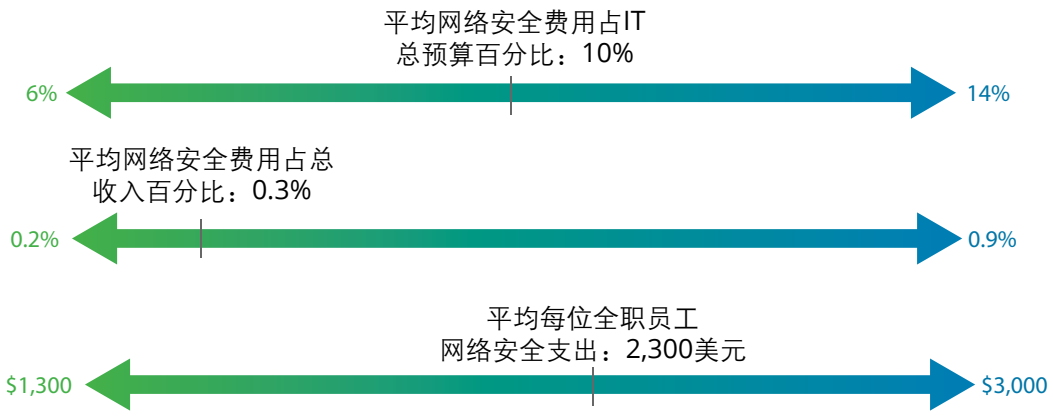
尽管小型企业全职员工人均网络安全支出2,100美元与中型企业相当，但远低于大型企业的2,700美元。这可能是因为大型企业组织架构较复杂，通常需要提供更多的产品和服务，并需要同时考虑多个业务部门和交付渠道。

接受调查的小型企业在IT预算中用于网络安全的比例(12%)高于大、中型企业(9%)。这或许表明小型企业意识到它们需要在网络安全方面加大投入力度，以满足网络安全监管要求和运营需求。

进一步对企业投入数据进行深入分析，我们发现大型企业将其约五分之一的网络安全开支用于身份和访问管理 – 这几乎是中小型企业的两倍；而中小型企业往往倾向在终端和网络安全上增加支出。（关于如何根据受访者的收入规模对其网络安全支出进行比较，请参阅第13-14页“企业规模决定差异化策略”。）

图4

金融机构平均网络安全支出（总样本）



注意：所有金额均以美元计算。

资料来源：2019年FS–ISAC/德勤网络风险服务CISO调查，德勤金融服务行业研究中心。

图5

金融机构平均网络安全支出，按企业规模分析

	小	中	大
网络安全费用占IT总预算百分比	12%	9%	9%
全职员工人均网络安全支出	$2,100	$2,100	$2,700
网络安全费用占总收入百分比	0.2%	0.5%	0.4%

注意：所有金额均以美元计算。
资料来源：2019年FS-ISAC/德勤网络风险服务CISO调查，德勤金融服务行业研究中心。

在金融行业的不同领域中，网络安全支出也存在差异。例如，银行业受访者表示，他们将约11%的IT预算用于网络安全，略高于行业平均水平；而保险和非银行金融服务公司在网络安全方面分配的预算低于行业平均水平 (10%) - 即便如此，不同领域对于网络安全分配的预算均为其整体收入的0.33%。就每位全职雇员人均网络安全支出而言，非银行金融服务公司支出金额大约为2,800美元，大于银行 (约2,000美元) 或保险公司 (约2,200美元) 。

调查样本中金融设施，如清算机构，交易所和结算公司，其网络安全预算投入最高，约占其整体IT预算的15%、总收入的0.75%、每位全职员工人均支出约3,600美元。服务提供商 (金融产品/服务/应用程序) 对网络安全的投入也较多，约占其IT总预算的11%和收入的0.60%。但每位全职员人均支出只有2,000美元左右，这一数字与银行业受访者大致相同。

尽管按照网络安全成熟度水平划分，不同成熟度企业的网络安全开支略有不同，但成熟度为自适应级公司在网络安全上的花费并不一定高于样本总体平均水平，这符合我们的核心主题即——网络安全工作如何计划、执行和治理与其资金投入同等重要。那么，成熟度最高的自适应级公司在其网络安全中所运用的管理与技术有何过人之处？

领先网络安全管理特征

CISO通过大量系统和流程来确保他们的企业免受网络入侵，建立高效的预警机制，以使他们在可能面临强大的网络威胁之前提早发现，并在遭受重大网络攻击时快速恢复。由于大量风险管控活动在同时进行，CISO有时会很难确定其工作的优先顺序。那么，应采取哪些基本手段来快速提升金融机构的网络安全成熟度，并持续保持较高水平？

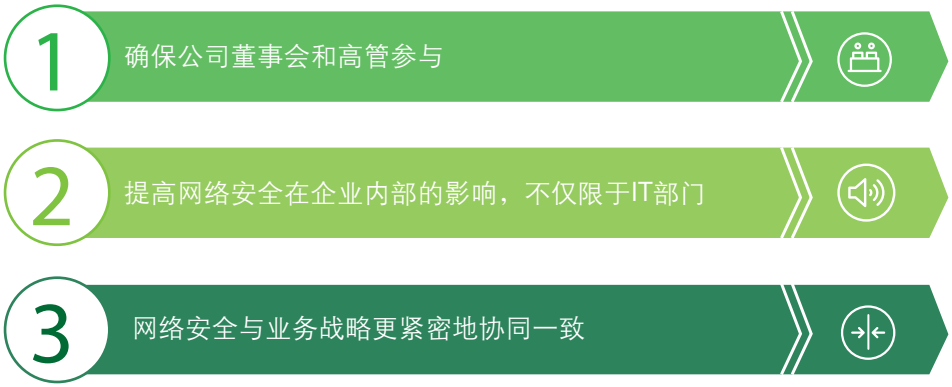
虽然促成网络安全工作成功的因素有很多，但与其他企业相较，领先的网络安全实践—自适应级企业具有三项主要特征，它们通常能够：1）确保公司董事会和高管参与；2）提升IT部门以外的其他各部门的整体网络安全意识；3）网络风险管理与业务战略结合更加紧密（图6）。

这些发现符合NIST对自适应级企业的描述。几乎所有归类为“自适应级”企业的受访者都进行了自评估，这意味着他们完全理解企业需要做到以上三点，才能达到最高的成熟度水平。

这些自适应级企业可作为其他成熟度较低组织的模板和参考，成功效仿这些特征的金融机构可在短期内提高其网络安全成熟度，并在长期内持续加强其网络防御能力。

图6

自适应级企业网络安全的三项特征



来源：德勤金融服务行业研究中心调研反馈

低成熟度企业通过效仿自适应级企业，还可以使CISO发挥其作为传统的技术专家和监护人角色以外的职能，使其同时作为战略专家和顾问投入更多时间，更好地支持业务部门、管理团队和董事会实现运营目标。[4]

特征一：董事会和管理层在网络安全方面的参与

NIST定义的具有自适应能力的企业，要求高级管理层将网络风险和财务风险以及其他企业风险给予同等程度的重视与监控。[5]

这与我们的调查结果一致，即缺乏管理层支持或资金不足是成熟度较低企业在管理网络安全方面所面临的最大挑战。

我们分析发现，除了高管以外，那些自评估成熟度在自适应级别的受访企业的董事会和管理层，对网络安全的关注不仅限于日常的工作汇报，而是几乎对网络安全的所有领域感兴趣（图7）。相比之下，网络安全成熟度最低的公司的董事会和管理层似乎对网络安全活动毫无兴趣。

图7

成熟度为自适应级企业，其董事会对网络安全活动参与度通常会更高

	自适应级	可重复级	可知晓级
总体安全战略	14	33	7
安全预算	6	19	6
安全政策	5	11	3
审查当前的威胁和安全风险	13	31	7
审查安全企业的角色和职责	3	6	0
审查安全测试结果	11	24	6
安全技术	3	5	1
项目进展	12	29	4
审查企业是否容易受到其他组织的公开攻击	11	27	5
其他	0	3	1
受访总数	17	43	14

来源：2019年FS-ISAC/德勤网络风险服务CISO调研，德勤金融服务行业研究中心。

网络安全独立于IT部门

相比之下，成熟度曲线上的可重复级企业，管理层对总体安全策略、威胁和安全风险审查、网络安全项目进展、安全漏洞、第三方泄露风险，以及安全测试结果审查有着更大的兴趣。在大多数领域，自适应级公司的董事会和管理层对网络安全尤为关注。

CISO和其他高管人员围绕当前威胁和安全风险，对其业务产生的影响，对董事会和管理层进行了大力宣贯，有助提升管理层参与度。设立一个与高级管理层就网络安全问题密切合作的委员会可以帮助整个企业集中精力应对挑战，确保为任务分配足够的资源。

我们的调研表明，在14家自适应级企业中，有5家将提升企业网络安全意识和进行相关培训列为高优先级事项；而在12家可知晓级企业中只有1家在这样做。提升网络安全意识与进行相关的培训无疑需要多个职能部门的资源和支持，更具自适应能力的公司往往能够更好地跨部门协调运作，将安全意识的实践嵌入到日常工作流程中，包括从新产品开发到客户服务等核心流程。

特征二：在IT部门以外提升网络安全影响

网络安全是起始于IT部门内的一项任务与关键职能。所有受访者中的一半（包括自适应级企业）报告说，安全团队在其企业中是IT职能的一部分，这并不奇怪。然而，企业的技术系统在大多数情况下已经不仅仅是网络攻击的目标，更逐渐成为企业防止入侵与及时止损的解决方案中尤为重要的一部分。

网络威胁越来越被认为是企业所面临的最关键的风险之一，今天的网络安全挑战也已经不仅仅是技术挑战。成熟度更高的公司已经认识到需要提高信息安全重要程度，从而在进行相关决策时，能够不受传统IT考虑因素的约束和禁锢。

调查结果（图8）显示，自适应级公司更有可能将网络安全从IT中分离出来，有效提升企业网络安全能力。可重复级公司正在努力将IT与网络安全职能分开，但仍保持共同的汇报路线。可知晓级的企业更倾向于将网络安全作为IT的一部分，并不打算将IT与网络安全分开，赋予其单独的身份。

大约一半自适应级企业（17个中的9个）实行完全独立的一道防线和二道防线，而在可知晓级企业中，14个中只有2个建立了独立的一、二道防线。

充分重视网络安全并将其与IT独立，也体现在自适应级企业的汇报路线中（图9），其中更多的CISO报告给首席运营官（COO）和首席风险官（CRO），而不是首席信息官（CIO）和首席技术官（CTO）。

调研还发现，几乎所有自适应级企业CISO的汇报级别不会低于首席执行官（CEO）两级；而在成熟度为可重复级企业中，3/4的汇报级别较低，成熟度可知晓级企业中，2/3的汇报级别偏低。

在整个调查样本中，很少有CISO向总法律顾问或CCO报告。这表明金融机构的大多数网络安全计划已远大于合规范围；他们正承担着更广泛的网络安全职能，负责打击网络风险，并且正在触及企业的每个角落。对于大多数积极主动的CISO而言，下一步可能是在业务规划和决策阶段提供战略支持。

图8

更成熟的网络安全管控模式正向着将网络安全从IT中独立出来的方向发展

	自适应级	可重复级	可知晓级
网络安全功能从IT职能中完全独立	4	5	1
IT和网络安全职能是独立的，但具有共同的报告线	1	10	2
IT和网络安全人员共同承担安全责任	3	11	1
网络安全职能是IT的一部分	9	17	10
受访总数	17	43	14

来源：2019年FS-ISAC／德勤网络风险服务CISO调研，德勤金融服务行业研究中心。

图9

首席信息安全官（CISO）或同等职能部门向谁报告？

	自适应级	可重复级	可知晓级
首席执行官（CEO）	2	5	2
首席财务官（CFO)*	1	1	1
首席信息官（CIO)*	2	10	7
首席技术官（CTO)*	1	5	0
首席风险官（CRO)*	4	6	0
首席合规官（CCO)*	0	0	1
首席运营官（COO)*	5	6	3
首席隐私官*	0	1	0
总法律顾问	1	3	0
其他	1	6	0
受访总数	17	43	14

*或同级别

来源：2019年FS-ISAC/德勤网络风险服务CISO调研，德勤金融服务行业研究中心。

特征三：网络安全与业务战略保持密切协同

在当今日益数字化、数据驱动的世界中，日常业务活动从内到外在很大程度上依赖于技术。只有企业利用新的技术创新、改变运营方式，才可以在众多竞争对手中脱颖而出。

然而，新的技术也可能使企业面临其他网络威胁。例如，大多数受访者表示，他们的企业计划在未来两年采用的两大新技术是云计算和数据分析。然而，正如德勤《2019年保险业展望》报告中所指出的那样，随着保险公司增加云的使用以加速转型和释放资源，监管机构一直在担心使用云可能导致的网络安全问题， 因为核心系统和关键数据基本上被移到了第三方。[6]虽然服务提供商对其硬件和软件的安全负责，但确保云安全这项工作的最终责任仍然在托管公司，任何第三方云安全方面的问题都可能对公司产生监管和声誉影响。[7]

银行CISO也经常面临类似的挑战。德勤《2019年全球银行业和资本市场展望》报告中指出“随着人工智能应用中使用的数据越来越多，对数据保护和隐私考量可能会使企业的风险管理复杂性升级”，“与第三方供应商的互联程度提高以及潜在的网络风险增加也是日益受到关切的问题。”[8]

自适应级企业似乎已经认识到网络安全需要与整体业务战略更紧密地联系在一起，他们意识到在管理网络安全的工作中，面临的第二大挑战是业务的增长与拓展（图10）。无论公司的成熟度如何，公司网络安全能力落后于快速变化和日益复杂的IT技术，是所有CISO面临的问题。随着企业通过增加新的平台、产品、地理区域、应用程序和网络功能来实现业务增长，每个新元素的引入都会使网络安全方面的考量成倍增加。

相比之下，网络安全管理成熟度较低的企业通常仍面临着更基本的问题，而不是如何应对业务增长所带来的挑战。例如，成熟度为可重复级企业面临的第二大问题是提升公司网络保护优先级，而成熟度为可知晓级企业面临的最大挑战是缺乏管理支持和资金不足。

将网络安全策略更好地与业务战略保持一致有助于CISO识别并应对新出现的风险。自适应级和可重复级企业的CISO认为，第三方/供应链控制缺陷是其面临的三大网络安全威胁之一。与此同时，成熟度为可知晓级企业似乎正在努力解决更多内部问题，例如未经授权的系统访问，网络风险检测和响应能力不足。

从一开始就将网络安全专业人员纳入战略计划和转型项目，将有助于安全职能部门更好地管理企业整体网络安全风险，促进企业内更大的合作和创新。[9]

图10

成熟度为自适应级企业更加意识到业务扩展对网络安全的影响

网络安全挑战排名

	总体	自适应级	可重复级	可知晓级
IT的快速变化和复杂度的增加	1	1	1	2
业务增长和扩张	2	2	4	5
更关注合规，较少关注网络风险管理	3	3	5	6
缺乏有经验的网络专业人员	4	6	3	4
难以确定保护企业的网络安全工作优先级	5	5	2	6
安全解决方案的功能性和互操作性不足	6	4	6	10
缺乏管理支持/资金不足	7	7	8	1
对网络风险和安全的理解不足	8	8	7	9
治理架构不充分	9	9	9	3
缺乏网络安全战略	10	10	10	8

来源：2019年FS-ISAC/德勤网络风险服务CISO调研，德勤金融服务行业研究中心。

持续提升网络安全成熟度

在审视金融机构的网络安全工作时，还有许多超出网络安全成熟度的其他因素考量，企业规模就是其中之一（参见附文“企业规模决定差异化策略”）；另一个则是企业所处行业。

然而，无论企业如何与其竞争对手相抗衡或开展竞争，网络安全仍是所有金融机构必须持续开展的一项工作。实际上，企业中无论谁最终对网络安全负责或者如何构建网络安全治理体系，网络安全意识、网络安全职责和对应的问责机制都应成为每个金融机构内部职能的一部分。

即使是网络安全成熟度较高的企业也应不断提升其网络安全的自适应能力

自适应级企业不应满足于其网络安全管理现状。虽然调研显示，成熟度较高的企业可能已经建立了稳固的治理体系，并打下了有效的网络风险管理基础，但为了保持对网络威胁的防御和响应能力，仍有许多工作要做。

如上所述，无论企业规模大小或成熟度高低，即使是自适应级企业，都在努力跟上IT快速发展的脚步和日益复杂化的技术系统，以保障其网络安全，这也被认为是CISO所面临的最大挑战。在这个消费者对数据安全和隐私保护高度敏感、监管要求层出不绝的时代，这些工作显得尤为迫切。

要想在网络安全领域取得卓越成绩将是一段曲折且没有终点的旅程。网络攻击将会变得更加严重和复杂，这要求金融机构具备更强大的响应能力。企业需要不断提升网络安全、人力和技术能力，从而达到保证网络安全、提前预警和遇到攻击快速恢复的目标。

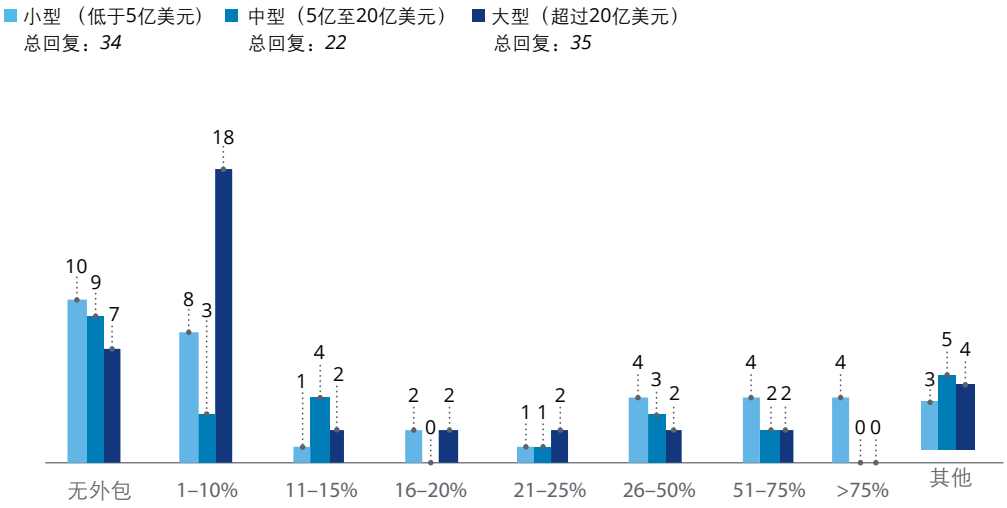
CISO也应不断积极主动的对潜在网络安全风险进行预测，时刻准备应对，而不是在出现新的攻击时再做出反应。如果没有采取有效的手段来提前防范网络安全风险，即使是自适应级企业，也很有可能在面对数字边界渗透和运营的攻击时变的不堪一击。

企业规模决定差异化策略

在我们的调研所提到的许多特征中，受访企业规模（按年收入）影响较大。 例如，企业规模较大的受访者更有可能将所有网络安全职能留在其内部，同样也最不可能将网络安全人员外包（图11）。

图11

网络安全人员外包百分比，按企业年收入进行排序



注意：所有金额均以美元计算。

来源：2019年FS-ISAC/德勤网络风险服务CISO调研，德勤金融服务行业研究中心。

规模较大的企业倾向于将其CISO设置在IT架构内部：56%的受访者表示他们的CISO向CIO或CTO汇报，而不是CRO或COO，而大约四分之一的中型和小型企业CISO向CRO或COO汇报（图12）。也许由于小型企业组织架构扁平化，来自小型企业的受访者最有可能让他们的CISO向CEO报告。与此同时，只有少数中型企业的受访者表示，他们CISO向公司高级管理层报告，这一现象在大企业中几乎不存在。

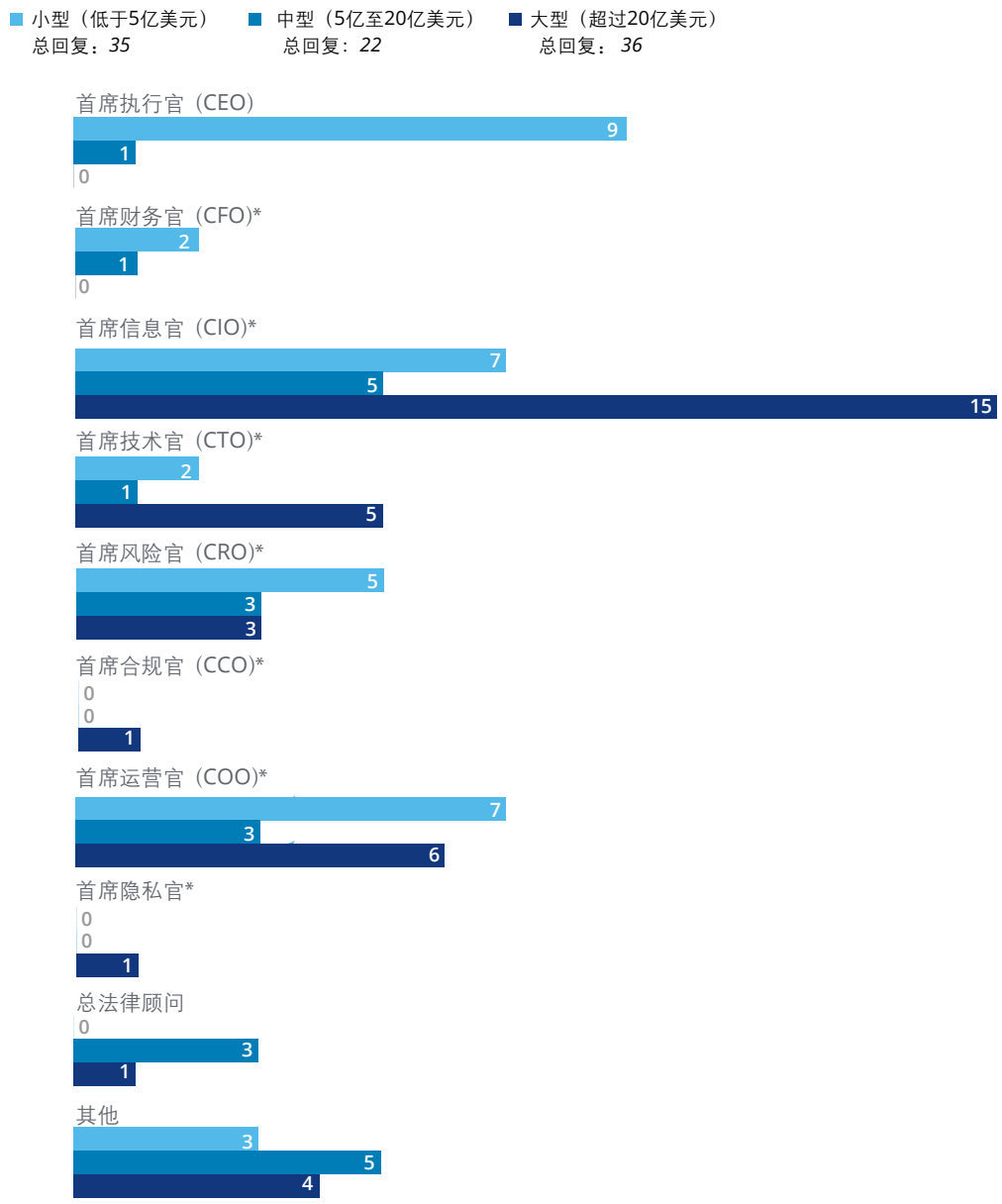
规模较大的企业受访者更有可能尝试混合运营模式，即在集权机构和单个业务线或地区都具有战略和执行能力。不管是在集权机构还是单个业务线，职能都是集成在一起并相互协调。然而，不论企业规模大小，这种做法仍是少数。只有十分之一的大型企业走这条路，这一比例在中、小型企业中更低。

大型企业也更有可能拥有独立的网络安全二道防线，并通过安全联络人或每个板块的“接口人”与企业建立网络安全接口。

风险转移是另一个使企业在网络安全层面产生差异的因素。受访者中只有不到十分之一的大型企业在没有网络安全保险的情况下运营，这一比例在中型企业中为四分之一。有网络安全保险的受访企业整体网络安全计划也相对较为成熟。 23家大型企业受访者中有8家表示他们的网络安全成熟度为自适应级，13家为可重复级，2家为可知晓级。20家中型企业中，只有2家处于自适应级，14家可重复级，4家可知晓级。 31家小型企业受访者中，有7家表示他们的网络安全成熟度为自适应级，16家可重复级，8家可知晓级。

图12

CISO向谁汇报，根据公司年收入划分



注：所有金额均以美元计算。

来源：2019 FS-ISAC/德勤网络风险服务CISO调研，德勤金融服务行业研究中心。

尾注

1. NIST, "Framework for improving critical infrastructure cybersecurity."
2. Jim Eckenrode and Sam Friedman, *The state of cybersecurity at financial institutions: There's no "one size fits all" approach*, Deloitte Insights, May 21, 2018.
3. National Institute of Standards and Technology (NIST), "Framework for improving critical infrastructure cybersecurity," April 16, 2018.
4. Khalid Kark, Monique Francois, and Taryn Aguas, "The new CISO: Leading the strategic security organization," *Deloitte Review* 19, July 25, 2016.
5. NIST, "Framework for improving critical infrastructure cybersecurity."
6. Sam Friedman et al., *2019 insurance outlook*, Deloitte, November 2018.
7. Ibid.
8. Val Srinivas et al., *2019 banking and capital markets outlook*, Deloitte, November 2018.
9. Deloitte, *The future of cyber survey 2019*, March 4, 2019.

联络我们

德勤中国联系人

方烨
德勤中国金融服务业
风险咨询领导合伙人（中国大陆）
+86 21 6141 1569
yefang@deloitte.com.cn

薛梓源
德勤中国
风险咨询网络安全合伙人
+86 10 8520 7315
tonxue@deloitte.com.cn

肖腾飞
德勤中国
风险咨询网络安全合伙人
+86 10 8512 5858
frankxiao@deloitte.com.cn

张震
德勤中国
风险咨询网络安全合伙人
+86 21 6141 1505
zhzhang@deloitte.com.cn

石沛恩
德勤中国
风险咨询网络安全合伙人
+86 21 3313 8366
nathanshih@deloitte.com.cn

何微
德勤中国
风险咨询网络安全合伙人
+86 755 3353 8697
vhe@deloitte.com.cn

郭仪雅
德勤中国
风险咨询网络安全合伙人
+852 2852 6304
evakwok@deloitte.com.hk

Tony Wood
德勤中国金融服务业
风险咨询领导合伙人（中国香港）
+852 2852 6602
tonywood@deloitte.com.hk

何晓明
德勤中国
风险咨询网络安全合伙人
+86 10 8512 5312
the@deloitte.com.cn

冯晔
德勤中国
风险咨询网络安全合伙人
+86 21 6141 1575
stefeng@deloitte.com.cn

江玮
德勤中国
风险咨询网络安全合伙人
+86 21 2312 7088
davidjiang@deloitte.com.cn

Puneet Kukreja
德勤中国
风险咨询网络安全合伙人
+86 21 3313 8338
puneetkukreja@deloitte.com.cn

Miro Pihkanen
德勤中国
风险咨询网络安全合伙人
+852 2852 6778
miropihkanen@deloitte.com.hk

海外联系人

Julie Bernard
Advisory principal
Cyber Risk Services
Deloitte & Touche LLP
+1 714 436 7350
juliebernard@deloitte.com

Kenny M. Smith
Vice chairman
US Financial Services Industry leader
Deloitte LLP
+1 415 783 6148
kesmith@deloitte.com

Sam Friedman
Insurance research leader
Deloitte Center for Financial Services
Deloitte Services LP
+1 212 436 5521
samfriedman@deloitte.com

Nikhil Gokhale
Insurance research manager
Deloitte Center for Financial Services
Deloitte Support Services India Private Limited