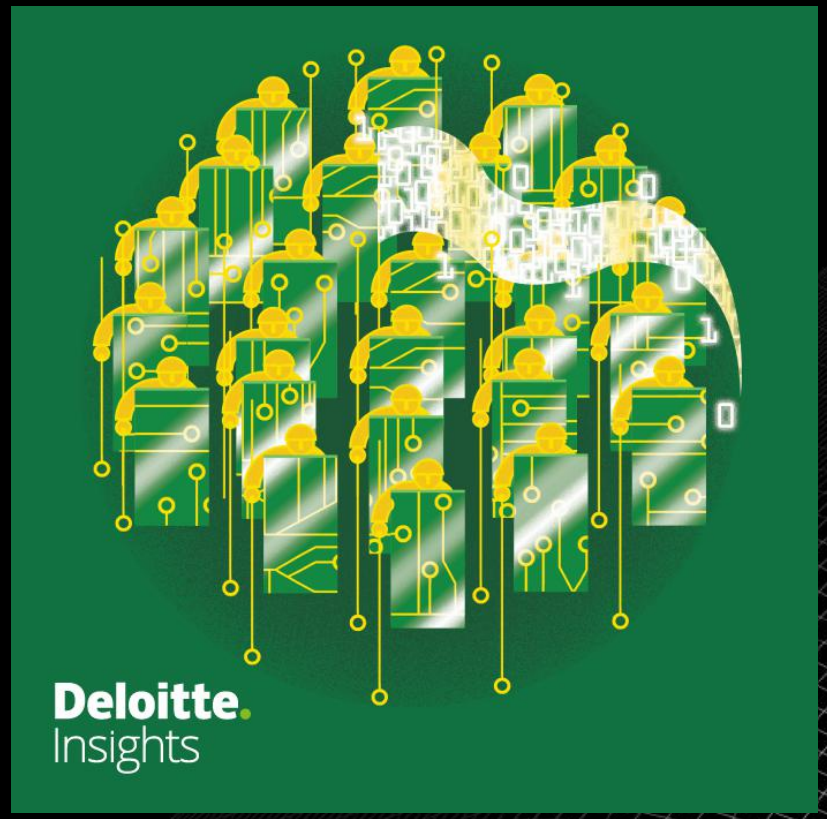
提升金融机构网络安全成熟度: 风险管理领先实践

马红杰　德勤中国风险咨询网络安全总监

CIS 网络安全创新大会
Cyber Security Innovation Summit

报告背景介绍

网络安全创新大会
Cyber Security Innovation Summit



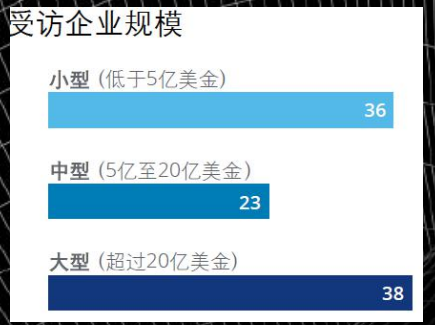
https://www2.deloitte.com/cn/zh/pages/financial-services/articles/pursuing-cybersecurity-maturity-at-financial-institutions.html

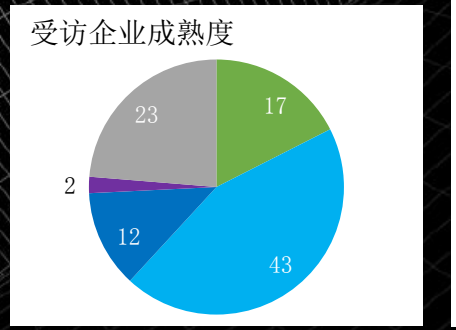
本调研由金融服务信息共享和分析中心（FS-ISAC）与德勤网络风险服务共同完成。FS-ISAC是一家总部位于美国的行业联盟，成员包括近7,000家金融机构，致力于降低全球金融体系中的网络风险。

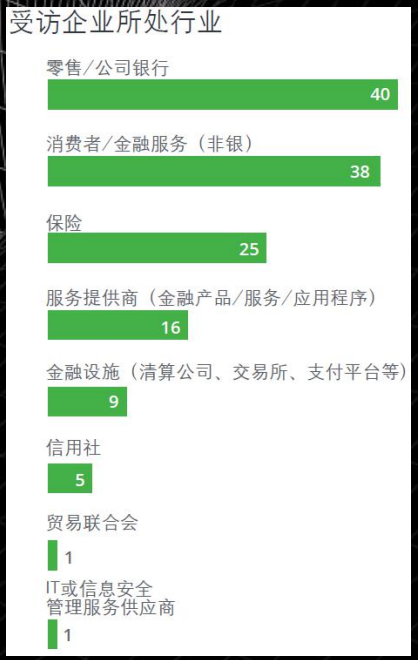
通过对FS-ISAC下97家成员单位的调研，就如何应对网络安全挑战进行调研，旨在评估各家网络安全预算和整体网络风险管理是否达到了良好状态。

本报告

- 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。







网络安全成熟度水平

- 2014年2月12日，美国国家标准技术研究院（NIST）正式发布了《提升关键基础设施网络安全的框架》第1.0版本。
- 2018年4月16日，美国国家标准与技术研究院（NIST）再次发布了《提升关键基础设施网络安全的框架》1.1版本。

该框架侧重于对美国国家与经济安全至关重要的行业，旨在形成一套适用于该领域的安全风险管控的“通用语言”，针对关键基础设施的安全风险管控的标准化实施给予指引，以帮助国家金融、能源、医疗保健等关键系统更好第保护其信息和资产安全，抵御网络攻击。

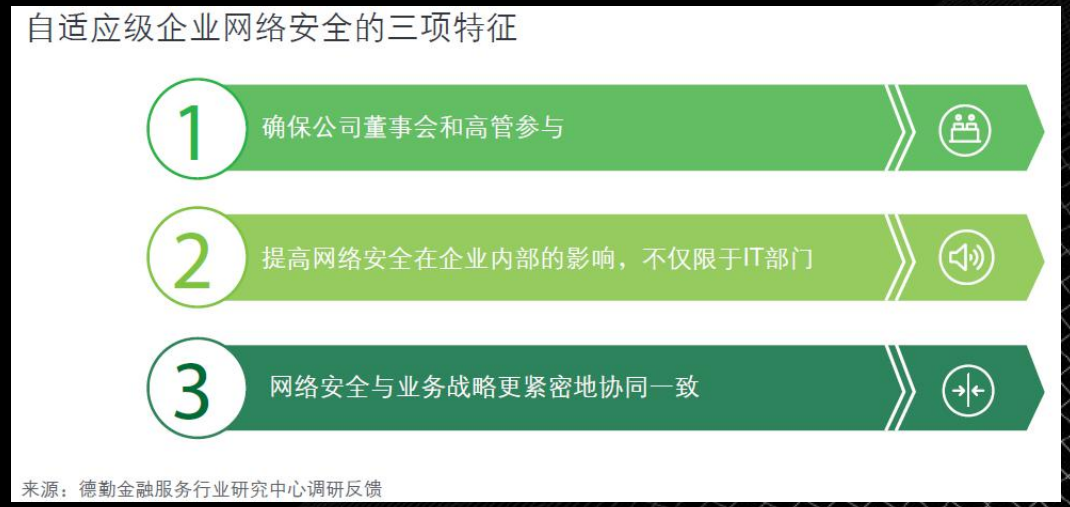
该框架强调用业务驱动引导网络安全活动，将网络安全风险作为组织风险管理流程的一部分。
在框架的框架执行层级为组织提供了评估网络安全风险的背景以及针对此种风险的现有管理流程。框架执行层级从低到高分为四级，1 级为“局部”，4 级为“自适应”，描述了网络安全风险管理实践的严格与复杂程度，以及网络风险管理受业务需求的影响程度及其与组织的总体风险管理实践的结合度。

初始级	（Partial）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	（Risk Informed）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	（Repeatable）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	（Adaptive）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：美，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

自适应级网络安全成熟水平的特征

NIST网络安全成熟度框架中所定义的“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。

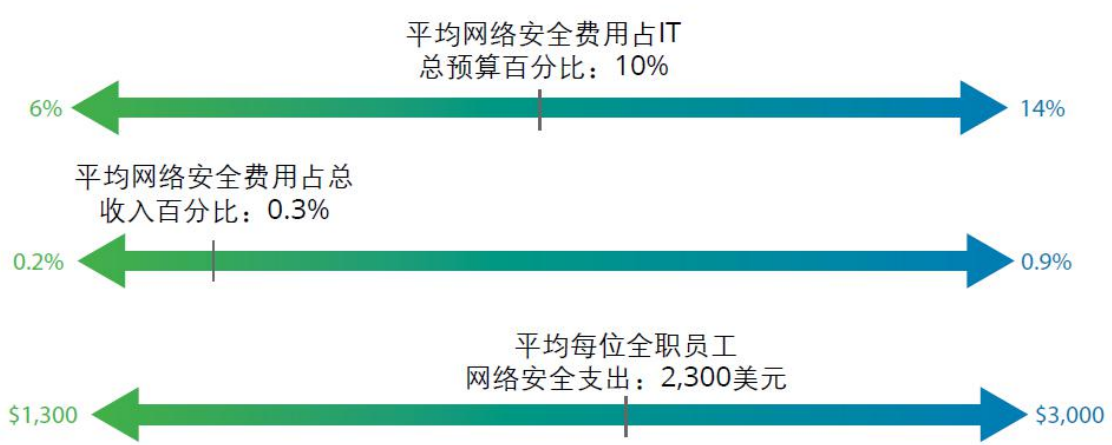
能够整合这些基本特征，并以网络安全行业领先实践为参考的组织，将更有可能适应不断变化的业务模式和应对来自日益白热化的外部竞争格局的威胁。

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

同行业不同特征的企业，在网络安全方面的投入，可以为网络安全及风险管理决策人员在安全预算及支出等方面，提供决策参考。

金融机构平均网络安全支出（总样本）



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%

不同规模的企业在网络安全领域的支出差异明显。

- 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
- 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

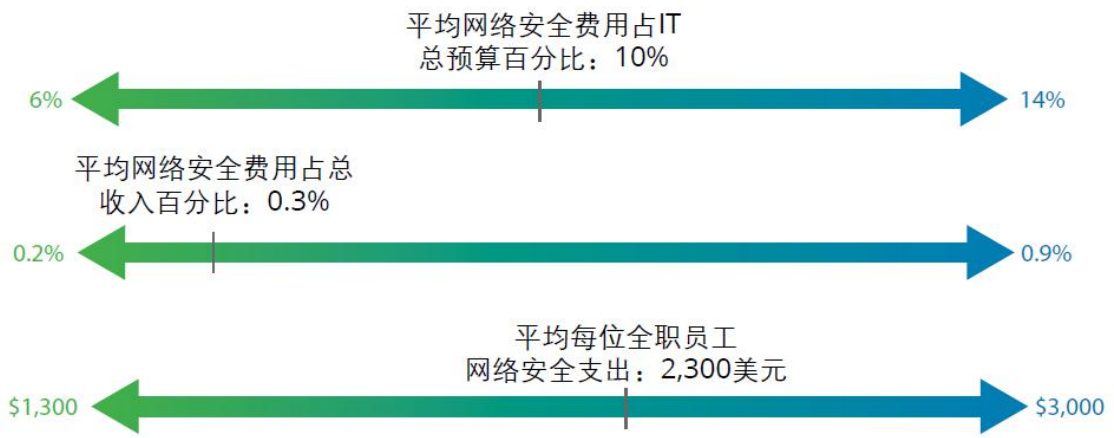
- 接受调查的小型企业在IT预算中用于网络安全的比例(12%)高于大、中型企业(9%)
- 小型企业已经意识到它们需要在网络安全方面加大投入力度，以满足网络安全监管要求和运营需求

- 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基础网络安全上增加支出

聚焦成本

同行业不同特征的企业，在网络安全方面的投入，可以为网络安全及风险管理决策人员在安全预算及支出等方面，提供决策参考。

金融机构平均网络安全支出（总样本）



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%

在金融行业的不同领域中，网络安全支出也存在差异。。

- 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；
- 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%）
- 金融设施机构（清算机构，交易所和结算公司等），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%
- 金融服务提供商（金融产品/服务/应用程序），约占其IT总预算的11%和收入的0.60%

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，
- 银行（约2,000美元）
- 保险公司（约2,200美元）
- 金融设施机构（约3600美元）
- 金融服务提供商（约2000美元）

- 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？

领先的网络安全管理的特征（一）

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。

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。
- 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。
- 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。
- 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。

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

- 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。
- 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。

领先的网络安全管理的特征（二）

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。

特征二：在IT部门以外提升网络安全影响。

- 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。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。
- 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。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

领先的网络安全管理的特征（二）

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。

特征二：在IT部门以外提升网络安全影响。

- 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）。

- 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。
- 在成熟度为可重复级企业中，3/4的汇报级别较低。
- 在成熟度可知晓级企业中，2/3的汇报级别偏低。

- 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。

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

领先的网络安全管理的特征（三）

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。然而，新的技术也可能使企业面临其他网络威胁。

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

- 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。
- 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。”

特征三：网络安全与业务战略保持密切协同

- 自适应级企业似乎已经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。
- 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。
- 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。
- 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

持续提升网络安全成熟度方面的建议

网络安全创新大会
Cyber Security Innovation Summit

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

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

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（例如“企业规模决定差异化策略”）；另一个则是企业所处行业。

- 安全战略：
  - 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。
- 安全组织：
  - 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。
- 风险策略：
  - 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
  - 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。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
- 安全实践：
  - 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

姓名　　马红杰

公司　　德勤中国

联系方式 jacma@deloitte.com.cn