Deloitte.

德勤

后疫情时代的网络安全：聚焦金融服务

因我不同
成就不凡
始于1845

目录

摘要

远程办公和**客户虚拟互动的**趋势将如何推动**数字化**发展并改变金融服务业网络安全格局？

- 有三分之二的受访者[1]表示，在2020年至2021年期间其所在企业经历了1至10起网络攻击和数据泄露事件。仅一起网络安全事件就可能使整个企业陷入瘫痪，并对企业声誉、财务状况或运营产生破坏。
- 远程办公的快速发展增加了企业面临的生态系统安全挑战，即从管理一个网络增加到数百个网络（具体取决于远程办公的员工规模）。
- 是时候淘汰传统系统，积极应用最新的工具和技术以提供高效的在线和移动服务，从而在市场中脱颖而出。
- 数据隐私和安全以及人才稀缺是企业仍犹豫将核心IT基础设施升级至云技术的关键原因[2]。
- 首席信息安全官应当拥有更大的权限去影响所有业务条线、收集整个企业范围内的信息并与董事会成员、高级管理层和利益相关者进行公开和坦诚的对话。
- 创造新金融科技解决方案的热潮伴随着网络攻击的显著增加，针对金融应用程序的攻击同比增长了38%。[3]
- 扩展企业风险是一个残酷的现实，企业需要做好相关规划。企业对于第三、第四和第五方的依赖性可能继续增强，因此对实时监控的需求亦有所增加。
- 人为错误仍然是头号网络安全威胁。安全意识培训仍是重中之重，但这还远远不够，打造网络安全文化至关重要。
- 首席执行官和董事会愈发重视更先进的风险量化技术，将其与更广泛业务风险联系起来。

新风险催生新措施

新冠疫情迫使许多员工进行远程办公，客户则要求几乎完全实现虚拟交互，金融机构不得不努力实现运营、分销和客户互动流程数字化。与此同时，网络安全专家也面临着迅速调整网络安全能力以应对不断变化的数字化需求的巨大挑战。

虽然疫情可能最终会有所缓解，但混合办公模式和数字化趋势必会继续存在，金融机构需要从长远角度出发，去考虑如何完善这些应对措施，金融服务业正致力于通过加强网络防御来实现这一目标。然而，通过优先考虑数字化转型计划、确保现代化活动的网络安全和建立有韧性的数字化运营以构建新发展格局仍任重而道远。

为了更好地了解企业如何应对这些新出现的压力，德勤调研了全球多个行业的近600名企业首席高管。[4]本报告聚焦金融机构（包括银行业及资本市场、保险业、投资管理和房地产行业），从首席高管们给出的162份回复中，我们分析得出了四个结论，金融服务业的管理层可以利用这些结论来构建其网络安全计划、确定投资优先事项并分配预算：

- 短期措施应迅速转化为长效机制
- 传统系统将逐步淘汰
- 扩展企业生态系统需要更强有力的监测和控制机制
- 有些事，亘古不变

在本文的后续部分，我们将更详细地逐一探讨上述结论。

短期措施应迅速转化为长效机制

受疫情影响，金融科技企业不得不加速推出多个项目以支持远程办公员工，协助各业务线提供数字化优先的产品和服务。为了跟上这些变化的步伐，企业需竭力适应完全不同的员工和客户互动模式，因此许多项目一直处于“测试或试点模式”。

现在，既然混合型员工队伍和虚拟交互将继续存在，那么就不能再停滞于测试阶段——企业需要确定将哪些变化纳入长期考量，又有哪些挑战仍有待解决。

担忧的理由

已有足够的证据表明，企业需要向新的稳定状态转变。在过去的一年里，网络安全事件激增。根据身份盗窃资源中心（ITRC）的数据，数据泄露事件在2020至2021年间增长了17%。[5] 67%的受访者表示，其所在企业在过去一年中经历了1至10起网络攻击或数据泄露事件，另有15%的受访者表示其所在企业经历了11至15起此类事件。

德勤《2021网络安全前瞻调研报告》亦支持上述发现。数据管理和边界保护的复杂性受远程办公增多的影响而不断加剧，已经成为影响金融服务业的最大挑战（图1）。

这与此前几年的情况形成鲜明对比。在过去几年中，企业普遍认为快速变化的技术是网络安全管理的首要挑战。[6]

刻不容缓

受访者着重指出了网络攻击事件增加的几个潜在原因，包括事件检测和响应能力不足、网络和终端资产太过复杂而难以保护、未能正确识别风险、网络安全治理和职责不清晰，以及员工未能遵守网络安全政策。

此前，企业通常使用端点检测与响应（EDR）以及安全监控来检测网络威胁。但随着全新运营模式的出现，企业需要更强有力的控制，包括严密监控访问控制并建立长期员工网络安全意识培训和合规性跟踪周期（包括返回办公室的员工和计划继续远程办公的员工）。

图1：贵企业在网络安全管理方面所面临的最大挑战是什么？

	所有金融服务行业	银行业及资本市场	保险业	投资管理	房地产
数据管理/边界和复杂性加剧	1	1	1	1	1
更好地确定企业网络风险管理的优先顺序	2	4	3	2	2
无法与快速的技术变革相匹配	3	2	2	3	5
缺乏网络风险专业人才	4	3	6	6	2
治理不足	5	5	4	4	4

资料来源：德勤《2021网络安全前瞻调研报告》

传统系统将逐步淘汰

虽然董事会和监管机构愈发重视网络安全，但随着全行业致力于提供高效的在线和移动服务并实现员工线上办公，IT团队需要进一步完善其基础设施。

从积极方面来看，大部分所需的数字生态系统均已到位，可以迅速扩展。但是，在这一基础上，我们的调研[7]结果表明，金融机构（尤其是大型机构）仍处于云技术应用的早期阶段。

完善核心基础设施

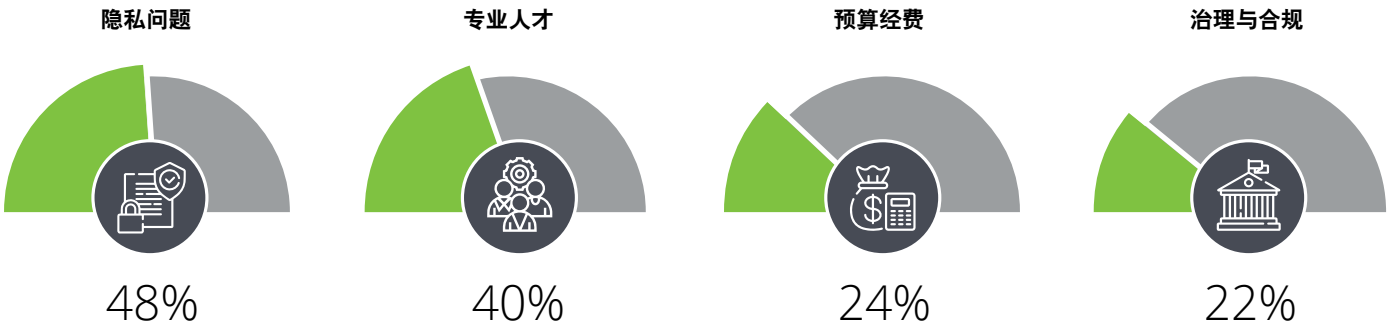
对踏上转型之旅犹豫不决的部分原因在于对全面采用云技术的持续担忧，包括隐私和人才稀缺（图2）。

同样，金融服务业受访者还表示，云环境的可见性和合规性是他们保护云应用程序和工作负载的首要考虑因素（图3）。

因此，企业应当评估云就绪状态的控制措施，尤其是许多企业在仅勉强满足现有要求的情况下，仍需要达到预期的控制目标并建立适用于云的控制措施。由于传统的安全管理实践通常无法跟上数字化转型的步伐进而导致控制漏洞、合规性失误和安全风险加剧，前述必要措施因此变得更加复杂。

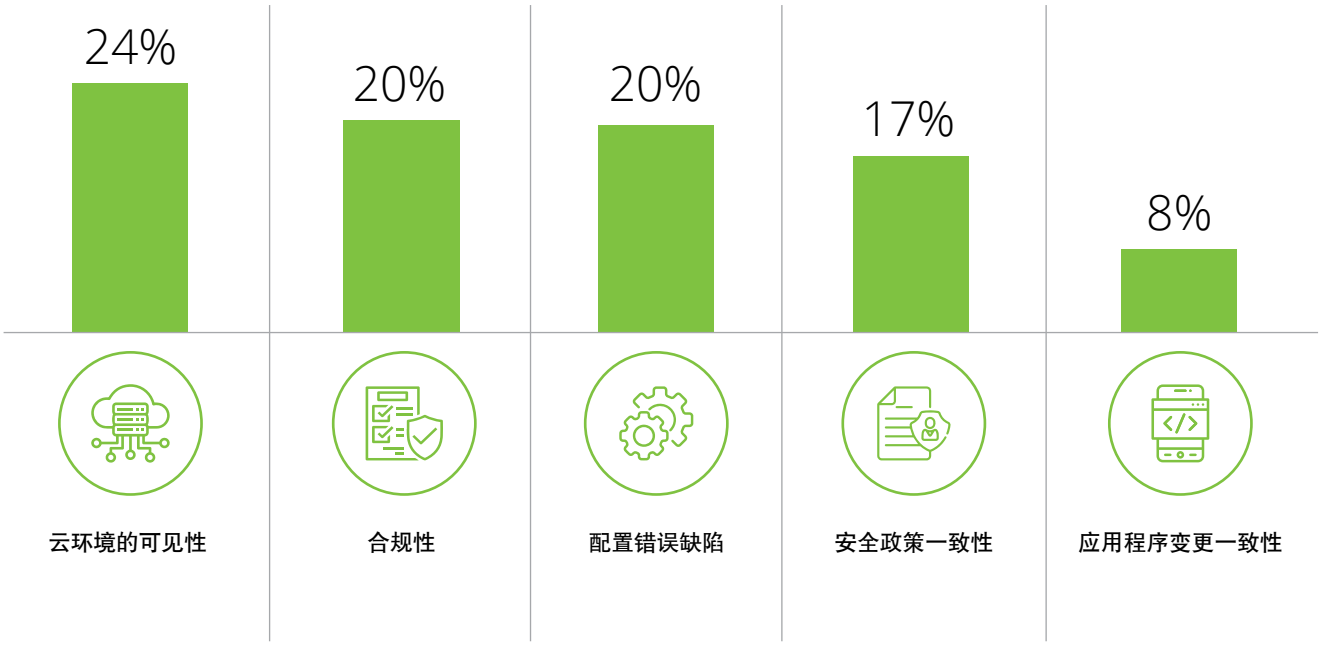
为应对这些挑战，企业需要加强业务部门之间的协调、实现控制和控制测试自动化，并提高评估更广泛的潜在风险（包括扩大的攻击面、第三方风险和功能成熟度）的能力。

图 2：下述什么类型的投资或要求会影响您对云安全的承诺？



资料来源：德勤《2021网络安全前瞻调研报告》

图3：在保护云应用程序或工作负载时，您最关心的问题是什么？



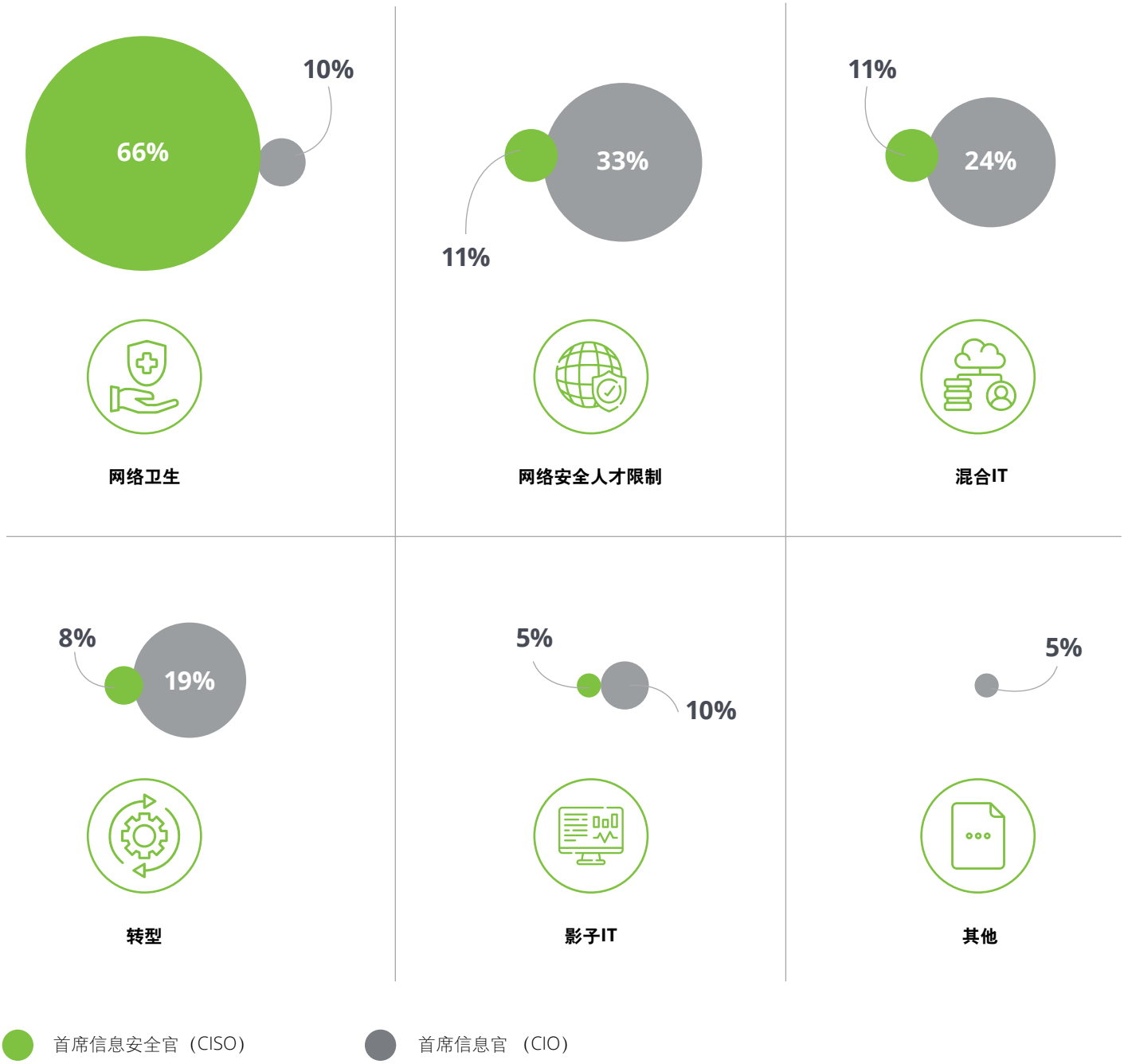
资料来源：德勤《2021网络安全前瞻调研报告》

完善网络基础设施

除关注核心系统以外，金融机构还应考虑改造其传统的网络安全基础设施。调研结果表明[8]，金融机构优先考虑通过云上规模化网络解决方案来提升其网络防御能力。例如，31%的受访者表示，其所在金融机构选择基于云端的身份即服务（IDaaS）解决方案，且更倾向于选择内部承包商采购、实施并提供持续的身份功能服务。

但企业的优先事项排序在因领导层看法不同而有所变化。66%的首席信息安全官（CISO）将网络健康（包括IT资产管理、配置管理、补丁和漏洞管理）视为企业网络安全管理最具挑战性的事项，而33%的首席信息官（CIO）则认为网络安全人才限制、混合IT和转型才是真正的挑战（图4）。

图4：以下哪项是贵企业在基础设施网络安全管理方面所面临的最大挑战?



资料来源：德勤有限公司，《2021网络安全前瞻调研报告》。

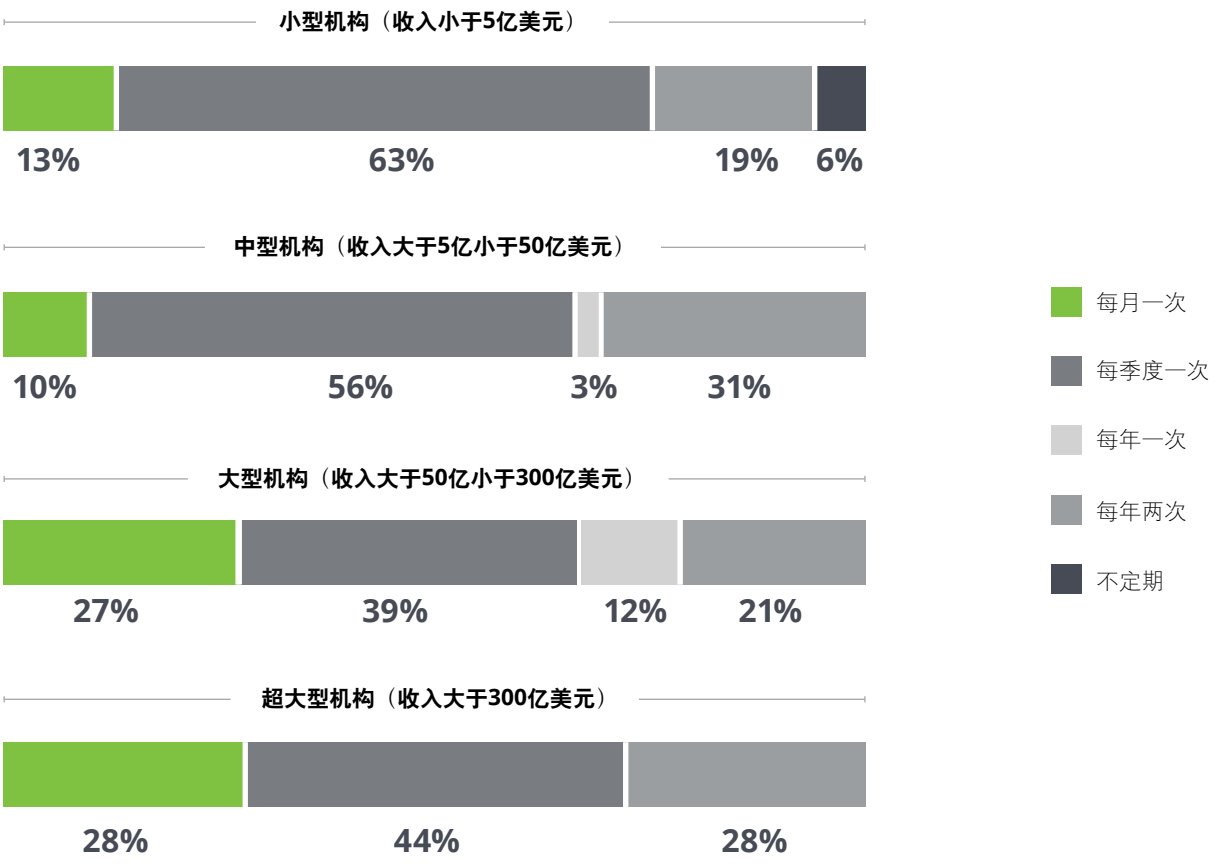
为应对这些挑战，首席信息安全官需要获得更多权限去影响所有业务条线、收集整个企业范围内的信息并与董事会和高级管理层直接对话。但这种必要性似乎因企业规模而异。在参与调研的超大型金融机构（收入大于300亿美元）中，28%的受访者表示其董事会每月都会讨论网络安全问题，而中型机构（收入5亿至50亿美元）中，仅有10%的受访者表示其董事会将网络安全问题列入月度会议议程（图5）。

显然，网络安全问题已经引起董事会的充分关注。如果首席信息安全官和网络安全团队想让董事会持续关注网络安全问题，需设法从一开始就将网络安全纳入产品设计和平台创新。

随着网络安全风险渗透至从客户触点到员工远程办公设备等各个方面，IT部门不能再孤军奋战，首席信息安全官也应将视线拓展至网络功能以外的方面。他们应做好准备，以恰当的方式，与三道防线中的董事会成员、高管以及利益相关者探讨其最担心的网络风险。

调研结果显示，首席信息安全官仍重点关注网络健康、 人才限制和混合IT（一种同时支持内部传统基础设施和公共云基础设施的技术）。由于网络安全专业人士仍仅在现有的基础设施中查漏补缺，所以这些问题仍然没有得到解决。为降低不断变化的网络风险，首席信息安全官应确定如何扩展关注范围，以开展更具战略性的开发、安全和运营（DevSecOps）举措。

图5：网络安全问题被提上董事会议程的频率是多少?



资料来源：德勤《2021网络安全前瞻调研报告》

扩展企业生态系统需要更强有力的监测和控制机制

虽然第三方风险管理是多年来的监管要求，但不断加速的趋势（如开放银行和金融科技关系等）更提高了这一要求。德勤金融服务行业研究中心的一项调研[9]发现，有五分之一的美国消费者认为开放银行业务具有价值，千禧一代和Z世代对此的兴趣尤为浓厚。传统金融机构和金融科技公司之间的关系已经改变了金融服务的建立、交付和消费方式，带来了前所未有的颠覆性变革和无限创新。

尽管优势明显，安全漏洞仍然存在。企业不断开发新的开放式应用程序接口（API）以连接银行和其他机构，引发了关于客户金融数据所有权的争论。而企业急于创建新的金融技术解决方案的同时，网络攻击数量也明显增多。仅在2021年上半年，针对金融应用程序的攻击就同比增长了38%。[10]

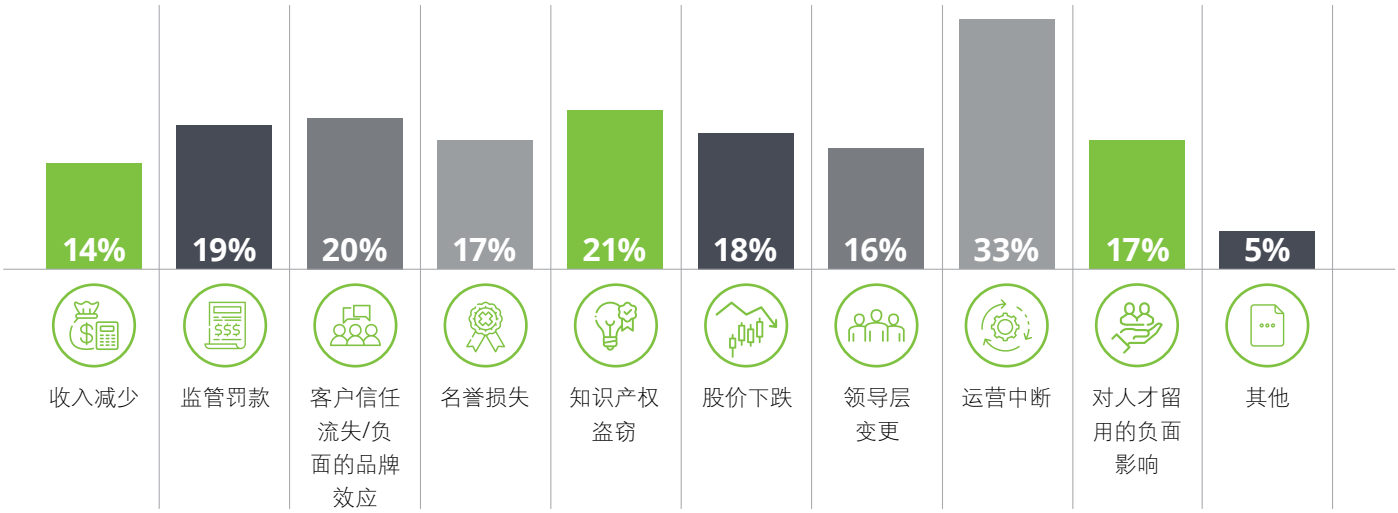
因此，网络安全专家面临更大的压力来保护更加以合作伙伴为中心且虚拟程度更高的企业。事实上，受访者认为，扩展企业的控制缺陷是如今许多金融机构面临的第二大威胁（去年被视为第三大威胁）。[11]

此处的“扩展企业”指支持金融机构和/或其客户的第三方供应商、提供商、代理商、经纪人和合作伙伴组成的扩展生态系统，如技术解决方案供应商、支付处理商、清算机构等。

网络事件的影响

扩展企业可能使金融机构面临更多的网络安全事件威胁。在被问及网络攻击和数据泄露的影响时，受访者[12]表示运营中断造成的影响最大（图6）。

图6：网络攻击和数据泄露给贵企业造成的最大影响是什么？（最多选择两项答案）



资料来源：德勤《2021网络安全前瞻调研报告》

强化控制环境

随着扩展企业的不断发展，零信任仍是必要实践——针对网络和应用程序、用户、设备和工作负载等信息访问应遵循最小授权原则。

零信任并非一种技术或单一的解决方案，而是一套基于“持续验证，从不轻信”这一原则的策略。其理念是将传统的基于边界或“城堡与护城河式”的安全管理方式，转变为按需在单个资源与客户之间构建信任的安全管理方式。在零信任模式下，用户将不断重新验证内外部因素以建立可信连接。

令人欣喜的是，受访者选择优先采用零信任框架，以及自动化和安全编排等网络防御措施（图7）。未来，金融服务机构还应进一步发展网络功能数字化，以提高敏捷性和速度。将安全设计原则纳入IT服务开发，并将网络安全要求嵌入软件开发生命周期架构和设计阶段，帮助金融机构提前应对不断变化的网络安全威胁。

图7：您将优先考虑/投资以下哪些网络防御概念以提升安全能力？

资料来源：德勤《2021网络安全前瞻调研报告》

有些事，亘古不变

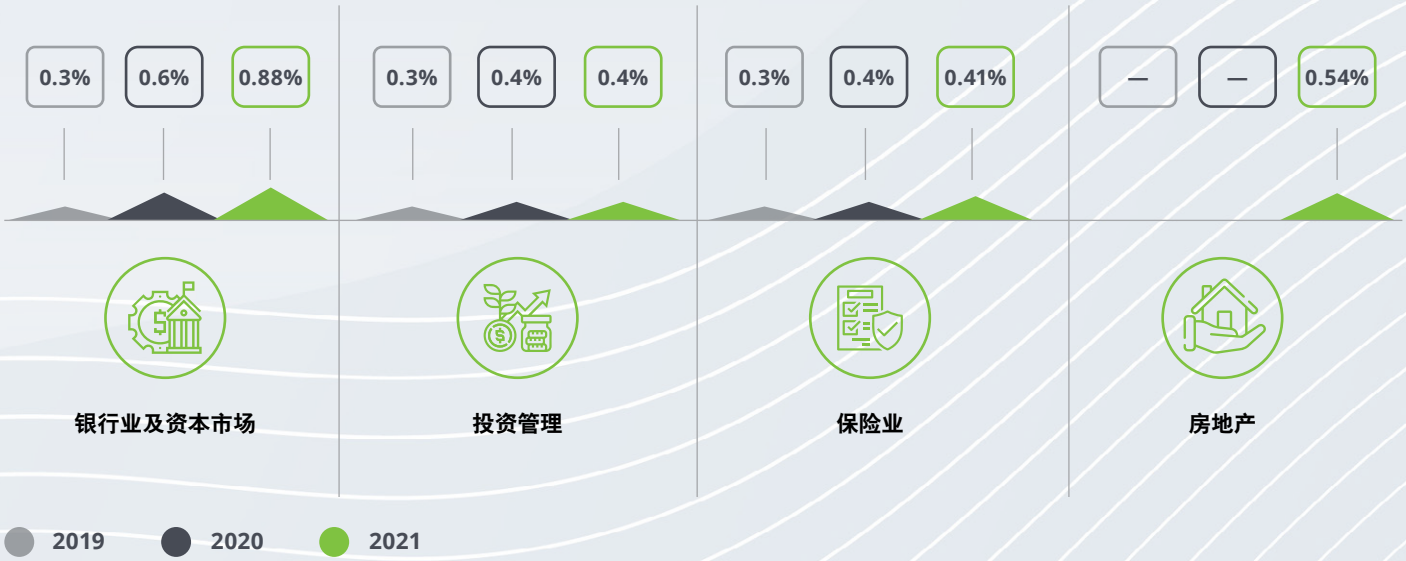
尽管环境多变，我们的调研[13]仍然强调了两个永恒的话题：企业投资网络安全管理的意愿，以及员工无法遵循常识性风险管理规定的情况。

就第一个话题而言，企业的网络安全措施预算仍然充足。过去的三年里，企业每年网络安全支出占年收入的比例不断增长（图8）。

2021年，基础设施安全、物联网（IoT）、工业控制系统（ICS）和运营技术（OT）共占据约20%的预算分配，其次是威胁情报、监测和监控（14%），以及网络转型（14%）（图9）。

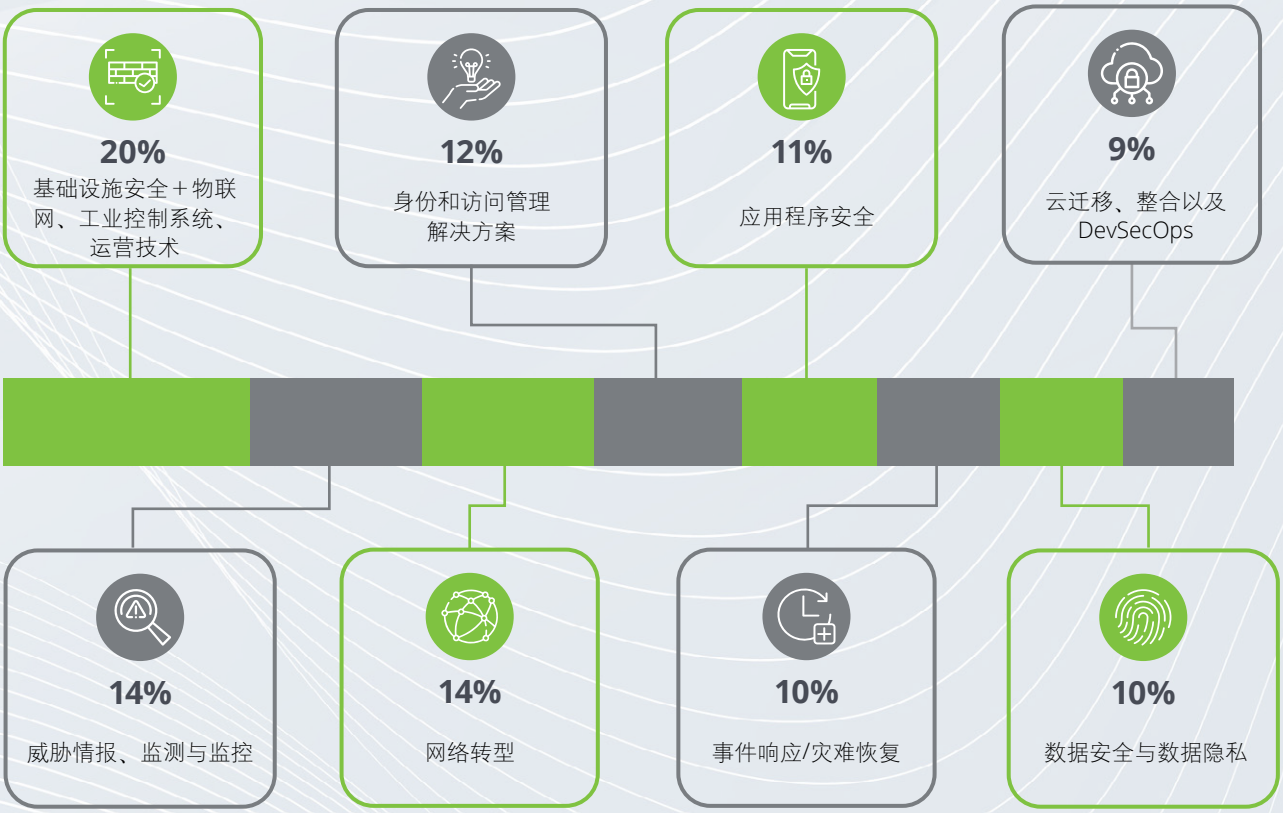
而在2020年的优先级排序中，19%的预算被分配给网络监控和运营、18%被分配给终端和网络安全、16%被分配给身份和访问管理。[14]首席信息安全官需要不断增加风险管理工具（包括采用风险量化技术）以实现网络安全投资收益。

图8：各部门网络安全支出和收入



资料来源：德勤《2021网络安全前瞻调研报告》；德勤与金融服务信息共享及分析中心（FS-ISAC）2019和2020年网络安全基准调研（Cyber Benchmarking Surveys）

图9：网络安全领域预算分配



资料来源：德勤《2021网络安全前瞻调研报告》

医者自医

虽然企业斥巨资实施网络安全管理，但人为错误仍然是头号威胁。受访者表示，网络钓鱼、恶意软件、勒索软件以及员工相关风险仍是网络安全面临的首要威胁（图10）。

多年来，尽管对这类威胁有所了解，但员工依然深受网络钓鱼、恶意软件和勒索软件之害，并持续通过无意行为或蓄意的恶意行为，为企业带来本可避免的风险。

虽然各企业正在制定应对这些威胁的韧性计划（图11），但此类计划通常更加注重响应和恢复，而非防御。培养员工对威胁的意识依旧是首要任务，但这仍然不够。

54%的受访网络安全专业人士表示，他们正在使用自动行为分析工具来监测员工的潜在风险指标，以进一步加强防御。25%的受访者表示将继续通过领导层来监测员工行为和风险指标，另有20%的受访者称其尚未找到方法来监测或缓减此类风险。

图10：根据企业的业务模式，您最关注的网络威胁是什么？

资料来源：德勤《2021网络安全前瞻调研报告》

图11：您已采取下列哪些措施来提升企业的网络和信息安全水平？

1

制定应对网络安全威胁的运营和战略计划

2

定期为所有员工开展网络安全意识培训

3

制定不断改进和发展企业网络和信息安全健康的流程

4

制定定期更新和测试的网络事件响应计划

5

定期听取客户对网络和数据隐私偏好的意见

资料来源：德勤《2021网络安全前瞻调研报告》

前路在何方

金融服务业的网络安全实践在不断完善；高管和董事会都将网络安全支出列为优先事项，并对新兴的网络安全协议进行投资，以确保其扩展企业免受不断扩散的网络威胁。即便如此，随着网络攻击方变得更加老练，首席信息安全官应不断重新审视其风险评估方法，以保持领先地位。根据我们的经验，首席信息安全官通常偏向于使用成熟度评估来确定支出优先事项，而首席执行官则更多地要求采用更复杂的风险量化技术，将更广泛业务风险联系起来。

在新冠疫情刺激下，数字化、远程办公和虚拟客户互动的发展速度惊人，首席信息安全官不得不重新审视其传统网络安全实践——从网络钓鱼和恶意软件到扩展企业控制缺陷和内部威胁，这些持续不断的威胁更加凸显了这一必要性。

随着远程办公以及数字化转型的发展，金融机构也应接受云技术，确保扩展企业的网络安全，专注于完善受信任客户体验，打造韧性运营并缩小控制差距。金融机构需要多管齐下，提升事件检测和响应能力，加强边界控制，改进风险识别方法，并实施更集中的员工教育措施。虽然对于整个行业的利益相关者来说，目前尚无可适用的万能解决方案，但风险的增加将继续迫使企业采取新的应对措施。

尾注

1. Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."
2. Ibid.
3. Ibid.
4. Ibid.
5. Identity Theft Resource Center, October 6, 2021. "Number of Data Breaches in 2021 Surpasses All of 2020."
6. Deloitte, July 24, 2020. "Reshaping the cybersecurity landscape."
7. Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."
8. Ibid.
9. Deloitte, October 21, 2019. "Executing the open banking strategy in the United States."
10. UpGuard, January 20, 2022. "The 6 Biggest Cyber Threats for Financial Services in 2022," by Edward Kost.
11. Deloitte Touche Tohmatsu Limited, "2021 Future of Cyber Survey."
12. Ibid.
13. Ibid.
14. Deloitte, July 24, 2020. "Reshaping the cybersecurity landscape."

报告原名 *Cybersecurity in a post-pandemic world: A focus on financial services*，由德勤美国网络安全团队撰写，德勤中国网络安全团队对报告进行了翻译。

联络我们

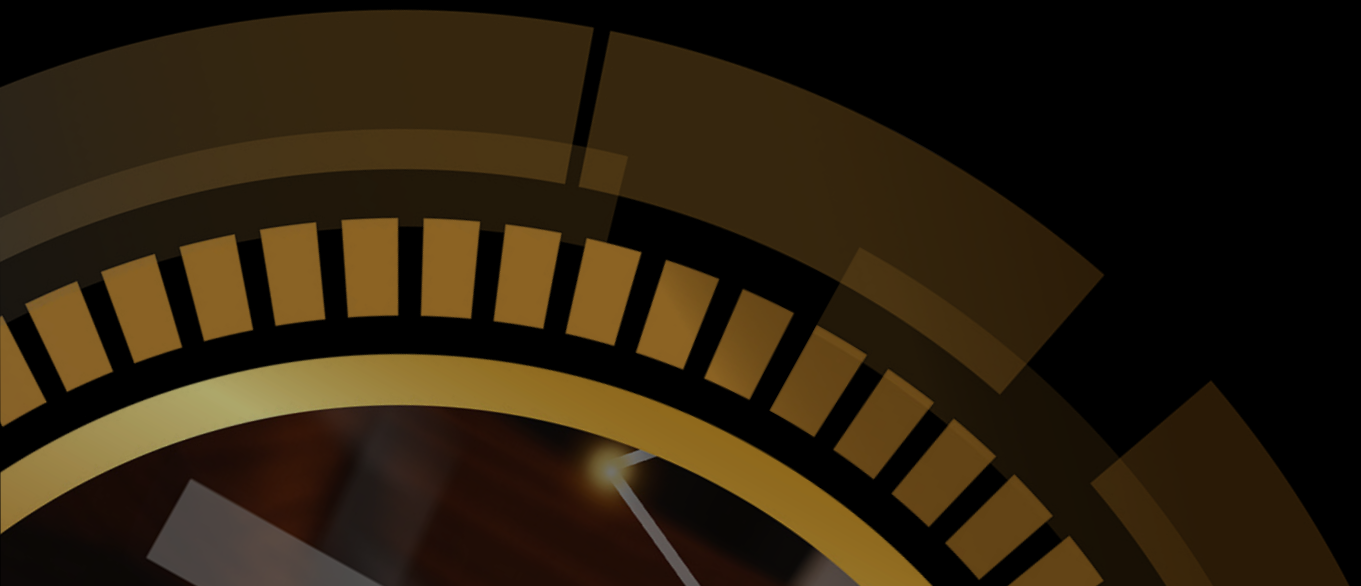
我们的专业洞察可助您充分利用和发挥变革的优势。如您正在寻求行业切入点以应对挑战，敬请与我们联系。

薛梓源
德勤中国风险咨询
网络安全与战略风险事业群主管合伙人
电话：+86 10 8520 7315
电子邮件：tonxue@deloitte.com.cn

冯晔
德勤中国风险咨询
网络安全与战略风险合伙人
电话：+86 21 6141 1575
电子邮件：stefeng@deloitte.com.cn

何晓明
德勤中国风险咨询
网络安全与战略风险合伙人
电话：+86 10 8512 5312
电子邮件：the@deloitte.com.cn

林松祥
德勤中国风险咨询
网络安全与战略风险合伙人
电话：+86 10 8512 4888
电子邮件：chaphylin@deloitte.com.cn



关于德勤

德勤中国是一家立足本土、连接全球的综合性专业服务机构，由德勤中国的合伙人共同拥有，始终服务于中国改革开放和经济建设的前沿。我们的办公室遍布中国30个城市，现有超过2万名专业人才，向客户提供审计及鉴证、管理咨询、财务咨询、风险咨询、税务与商务咨询等全球领先的一站式专业服务。

我们诚信为本，坚守质量，勇于创新，以卓越的专业能力、丰富的行业洞察和智慧的技术解决方案，助力各行各业的客户与合作伙伴把握机遇，应对挑战，实现世界一流的高质量发展目标。

德勤品牌始于1845年，其中文名称“德勤”于1978年起用，寓意“敬德修业，业精于勤”。德勤专业网络的成员机构遍布150多个国家或地区，以“因我不同，成就不凡”为宗旨，为资本市场增强公众信任，为客户转型升级赋能，为人才激活迎接未来的能力，为更繁荣的经济、更公平的社会和可持续的世界而开拓前行。

Deloitte（“德勤”）泛指一家或多家德勤有限公司，以及其全球成员所网络和它们的关联机构（统称为“德勤组织”）。德勤有限公司（又称“德勤全球”）及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体，相互之间不因第三方而承担任何责任或约束对方。德勤有限公司及其每一家成员所和它们的关联机构仅对自身行为承担责任，而对相互的行为不承担任何法律责任。德勤有限公司并不向客户提供服务。

德勤亚太有限公司（即一家担保有限公司）是德勤有限公司的成员所。德勤亚太有限公司的每一家成员及其关联机构均为具有独立法律地位的法律实体，在亚太地区超过100座城市提供专业服务。

请参阅 http://www.deloitte.com/cn/about 了解更多信息。

Designed by CoRe Creative Services. RITM1152475

这是环保纸印刷品