Ponemon INSTITUTE

金融服务业软件安全状况

独立调查

SYNOPSYS®

Ponemon Institute LLC
开展的调查

Created by CyRC

目录

关于本报告 1

概述 2

调查结果详述 4

金融服务公司的软件安全态势 4

金融软件和应用程序的风险 8

金融服务技术设计与开发的安全实践 12

结论和建议 18

风险和风险控制策略 18

利用托管服务来补充内部资源 19

方法 20

附录：具体调研结果 23

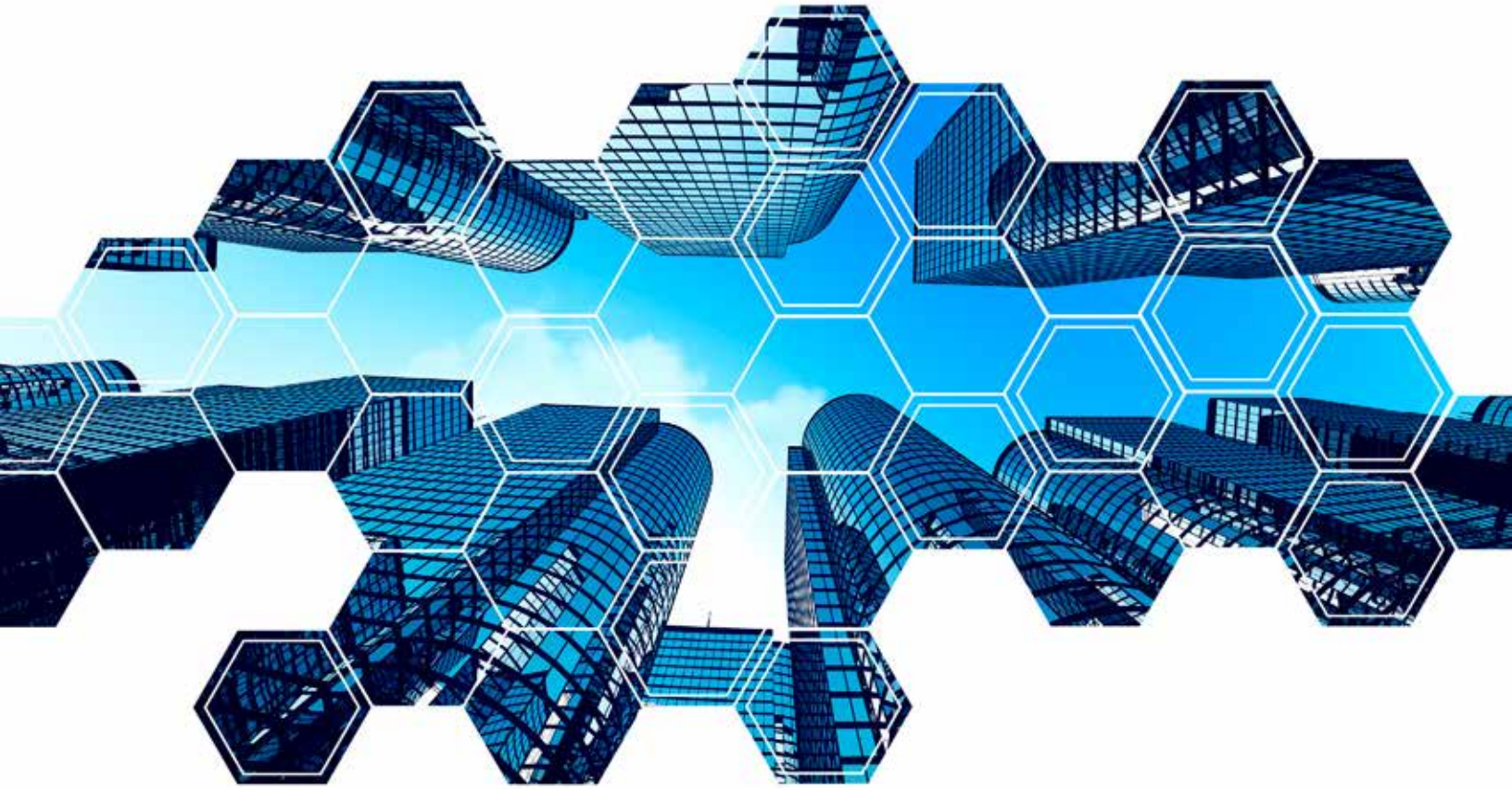
关于 Ponemon Institute 36

关于本报告

新思科技网络安全研究中心 (CyRC) 最近委托数据安全中心 Ponemon Institute 对金融服务行业 (FSI) 当前的软件安全实践进行独立调查，以了解该行业的软件安全态势及其解决安全相关问题的能力。这份名为《金融服务业软件安全状况》(SS-FSI) 的报告就是本次调研的结果。

为助力新思科技实现确保软件安全和高质量运行的目标，CyRC 会定期发布调研报告来支持强有力的网络安全实践。这些出版物包括深入洞悉开源代码在商业软件中的安全性、合规性和代码质量风险的年度报告《开源安全与风险分析 (OSSRA)》，以及 Synopsys 与 SAE International 为解决基于软件的联网车辆中固有软件安全风险而联合发布的报告《保护现代车辆的安全》。

为了撰写这份 SS-FSI 报告，Ponemon 的研究人员调查了来自金融服务行业各个领域的 400 多名 IT 安全从业人员，包括银行、保险、抵押贷款 / 处理和经纪领域。调研参与者来自各行各业的工作岗位，如安装和实施金融应用、开发金融应用以及为金融服务业提供服务等。有关本次调研方法和参与者的完整信息，请参见**“方法”**和**“附录”**部分。



简介

当前，大量新兴技术正涌向金融服务行业，其中最引人注目的是提高金融服务行业内部流程的自动化水平以提升效率和利润率，以及开发新的软件以便用户能在传统银行、网上银行和手机银行领域实现完整无缝的客户体验。

金融技术已深深地嵌入到每一项 FSI 业务中，如果没有它，任何银行或保险公司都将无法运营。但是，正如这份报告所显示的，大多数 FSI 机构都难以保护其现有技术。在参与本次调研的 FSI 机构中，超过一半 FSI 都曾经历因网络攻击而导致客户数据被盗、系统故障与宕机等安全问题。。

显然，FSI 现有的网络安全体系和技术已经跟不上金融服务业技术快速发展的步伐，如果不立即采取积极有效的措施，这个问题只会进一步恶化。

对 FSI 而言，网络安全是一个非常现实的问题

我们的报告显示，FSI 机构需要更多地关注网络安全、安全编码培训、用于发现源代码缺陷和安全漏洞的自动化工具、以及用于识别由内部开发团队和外部软件供应商引入的开源组件的分析工具（SCA）。

虽然 FSI 机构仍在持续构建所需的软件安全技能和资源，大多数机构都为软件开发人员提供了一定形式的安全开发培训，但是只有一小部分开发人员真正需要（或被强制参加）这种培训。此外，对于评估安全研发的效果，FSI 机构更多地依赖于内部评估，而不是使用 BSIMM（软件安全构建成熟度模型）或 SAMM（软件保障成熟度模型）等外部评估工具。

造成软件漏洞的最常见原因是开展漏洞测试在整个软件研发过程中为时过晚。我们发现，多数 FSI 机构往往在产品发布后才进行漏洞评估，可能出于诸多原因例如缺乏应用程序安全专业知识、担心成本问题、以及担心在软件开发生命周期 (SDLC) 过早地引入安全流程和安全活动会阻碍开发工作导致对市场的响应迟缓等等。

不到一半的受访者表示，安全评估发生在软件设计、开发和测试期间，只有 25% 的受访者表示，他们的机构能够在软件发布之前检测出金融软件和系统中的安全漏洞。

FSI 软件供应链是主要风险所在地

虽然大多数的 FSI 机构仍在自行研发软件和系统，但许多机构已经开始依赖第三方独立提供商来交付最新技术。尽管在本次调研中，近四分之三的受访者表示十分担心第三方软件供应商会带来安全漏洞，但只有不到一半的机构要求第三方软件供应商遵循特定的网络安全要求或验证其安全实践。

在参与调研的 FSI 机构中，几乎没有任何机构建立了相应的流程来录入和管理内部开发团队或由第三方软件供应商引入的开源代码。开源组件缺乏管理，应用程序中的开源组件存在漏洞，从而将 FSI 机构暴露在这些额外的安全风险之中。

保护 FSI 软件和系统没有统一的方法可循

没有任何一种方法、工具或服务能够确保任何 FSI 机构的绝对完全。

一些机构更喜欢依赖和利用托管服务提供商的安全团队，其他机构则更喜欢内部拥有丰富安全专业知识大型安全团队。

一些机构使用自动化工具的分层方法，包括 SCA（软件组成分析）、SAST、IAST 和 DAST（静态、交互式和动态应用安全性测试），以及 RASP（运行时应用程序自我保护）。其他机构的策略包括手工规划与测试活动，如安全架构设计、安全需求定义、威胁建模、代码审查和模糊测试等，以确保 SDLC 每个阶段的安全性。

唯一正确的方法是与业务保持一致，支持和保护业务。本报告中的数据揭示了一个有趣的事实，大多数的受访者都认为，其机构主要集中建设和提升网络攻击检测和攻击控制能力，而不是预防和阻止这些网络攻击。随着安全的更加关注，特别是将安全尽早融入到 SDLC 流程中，FSI 机构将有更好的机会来预防攻击，而不是处理这些攻击带来的后果和损失。

调查结果详述

本节将更深入探讨调研结果，分为以下几个主题：

- 金融服务公司的软件安全态势
- 金融软件和应用程序的风险
- 金融服务软件技术设计与开发的安全实践

完整审计调研结果在“附录”中呈现

金融服务公司的软件安全态势

FSI 机构更担心由第三方供应商提供的软件和系统的安全，而不是他们自己开发的软件和系统。

大多数的金融服务机构都在使用第三方供应商提供的金融软件和系统，同时自行开发金融软件和系统。虽然绝大多数的受访者都担心第三方引入的安全漏洞（见图 1），但只有 43% 的受访者表示，他们的机构要求第三方遵守网络安全要求或验证其安全实践。

图 1. 您对贵机构自行开发或由第三方提供的金融软件和系统的网络安全状况有多担心？

此处显示的是给出 7-10 分的受访者比例，计分从 1 到 10，1 = 毫不担心 ，10 = 非常担心

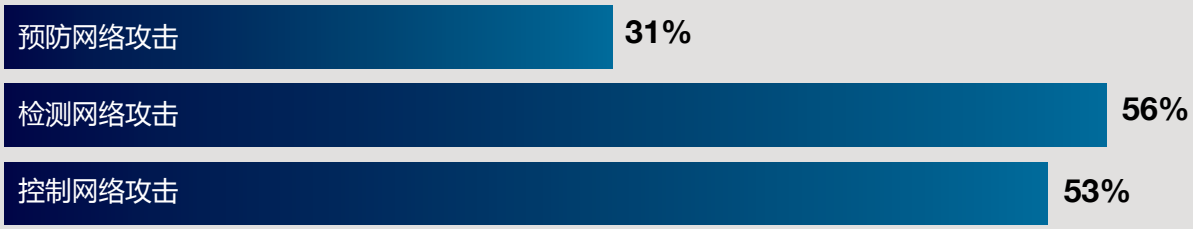
受访者认为，其机构的网络攻击检测和控制能力，要强于攻击预防能力。

受访者被要求评估其机构在预防、检测和控制网络攻击方面的效力。计分从 1 到 10，1 = 没效果，10 = 非常有效。

如图 2 所示，大多数受访者对其机构在检测和控制攻击方面的有效性充满信心，但在预防攻击方面则较弱。

图 2. 您的机构在预防、检测和控制网络攻击方面成效如何？

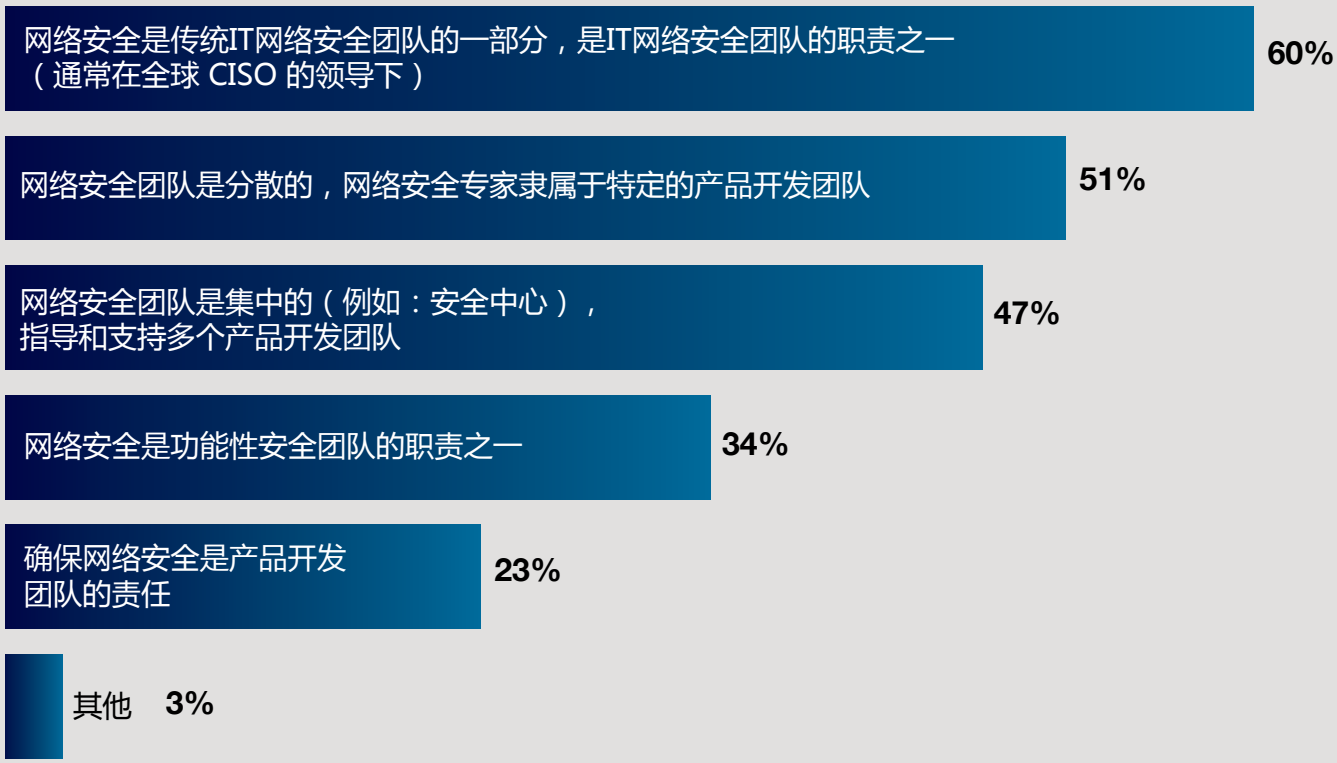
此处显示的是给出 7-10 分的受访者比例，计分从 1 到 10， 1 = 没效果，10 = 非常有效



大多数的 FSI 机构都拥有传统的 IT 网络安全项目或团队。

67% 的受访者表示，他们的机构拥有网络安全项目或团队。如图 3 所示，60% 的受访者表示，确保网络安全是传统 IT 网络安全团队的职责之一，超过半数 (51%) 的受访者表示，他们的网络安全团队是分散的，网络安全专家隶属于特定的产品开发团队。只有 23% 的受访者认为确保网络安全是产品开发部门的责任。

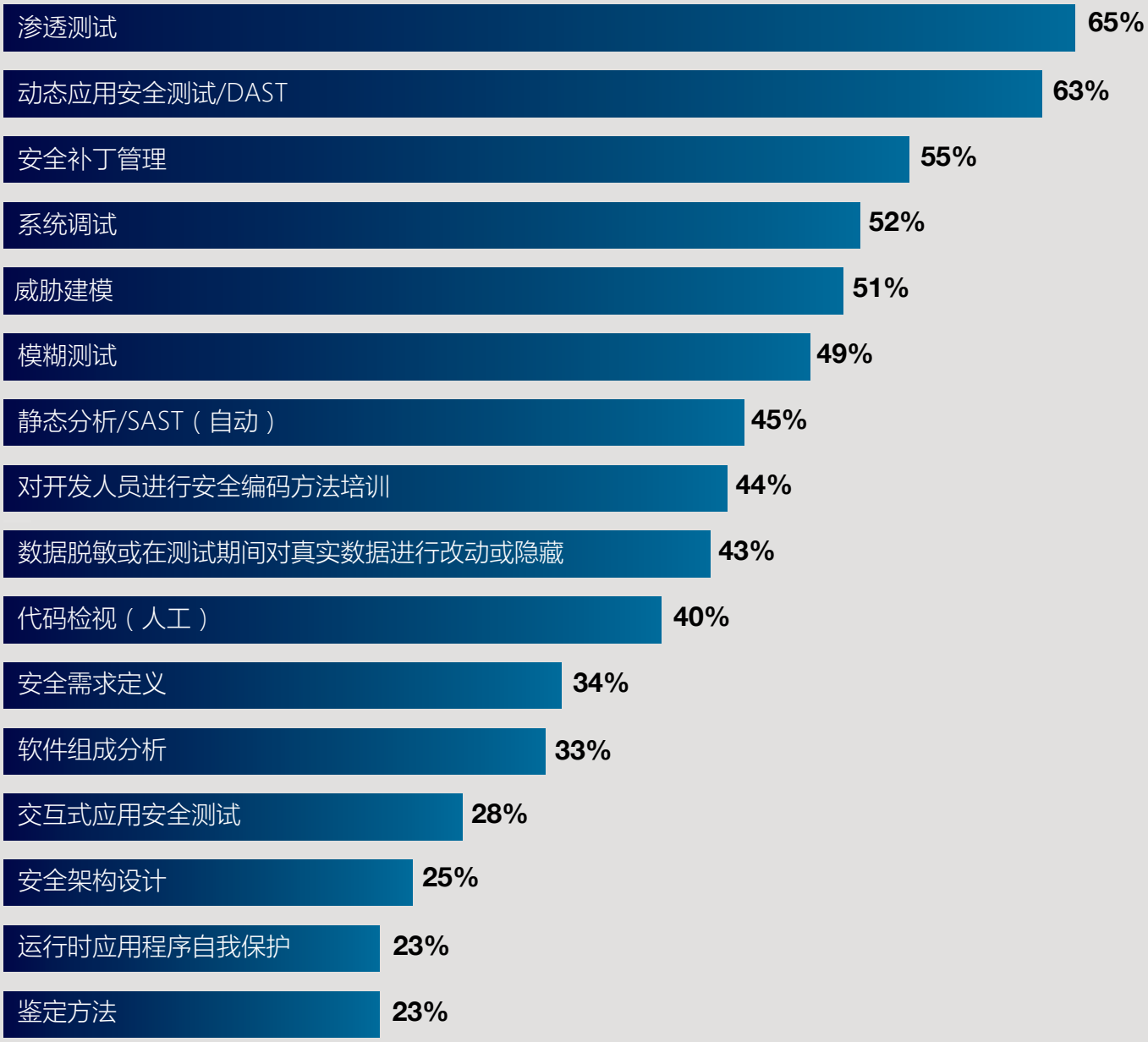
图 3. 贵机构如何处理网络安全问题？
67% 的受访者表示，其所在机构拥有网络安全项目或团队
可多选



受访者认为，渗透测试和动态安全测试 (DAST) 是降低网络安全风险最有效的方法。

65% 的受访者认为渗透测试、63% 的受访者认为动态安全测试 (DAST) 是降低网络安全风险最有效的活动。受访者还指出，安全补丁管理、系统调试和威胁建模也很有效。

图4. 哪些举措对降低网络攻击风险最有效？
可多选



受访者认为，他们的机构需要更多的资源和内部专业知识来消减降低网络安全风险。

如图 5 所示，只有 45% 的受访者表示，他们的机构有足够的预算来应对网络安全风险，只有 38% 的受访者表示，他们的机构拥有必要的网络安全技能。

图5. 我的机构为网络安全分配了足够的资源，并具备必要的网络安全技能

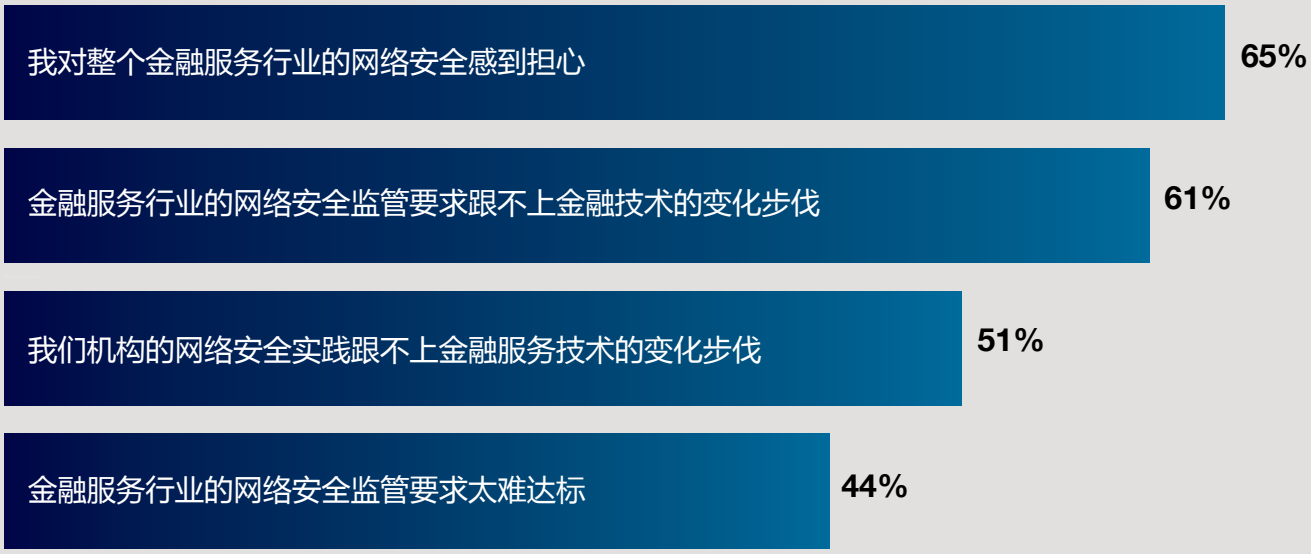
此处显示的是对此表示“强烈同意”和“同意”的受访者比例

受访者更担心金融服务业的网络安全状况，而不是合规难度。

受访者被要求在 1 至 10 分的范围内表达他们对网络安全风险的担心，其中 1= 毫不担心，10= 非常担心。图 6 显示了回答“非常担心”的受访者比例（10 分制，给出 7-10 分的受访者比例）。调研显示，65% 的受访者非常担心金融服务业的网络安全状况。尽管存在诸如《纽约金融服务局 (NYDFS) 网络安全条例》等新规定，仍有 61% 的受访者表示，金融服务业的监管要求跟不上例如区块链和开放银行 API 等金融技术的变化步伐。

图6. 对金融服务网络安全的担心情况

此处显示的是给出7-10分的受访者比例，计分从1到10， 1 = 毫不担心，10 = 非常担心



金融软件和应用程序的风险

受访者认为，云迁移工具带来最大的网络安全风险。

图 7 显示了受访者认为对金融服务公司构成最大网络安全风险的软件和技术。如图所示，60% 的受访者表示是云迁移工具，其次是区块链工具 (52%)

图7. 哪些软件和技术对金融服务公司的网络安全风险最大?

可多选

恶意行为者的威胁正促使企业在金融软件和技术领域实施与网络安全相关的控制。

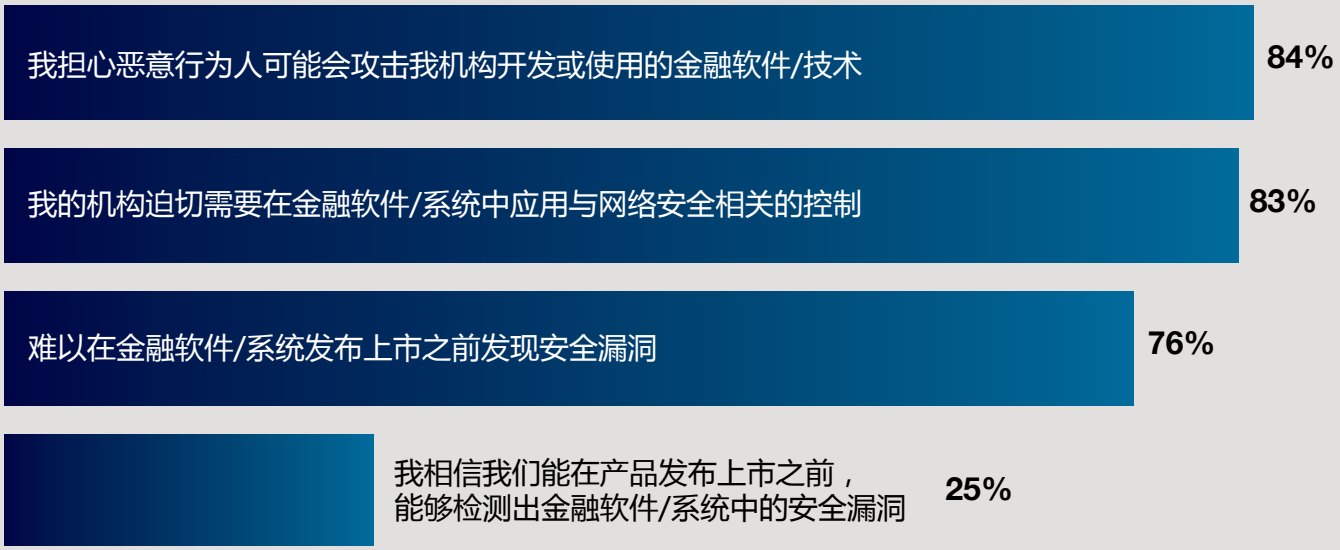
如图 8 所示 ,84% 的受访者表示 ,他们的机构非常担心恶意行为者可能会攻击他们所开发或使用的金融软件和技术(给出 7-10 分的受访者比例，10 分制，1= 毫不担心，10= 非常担心) 。

攻击面通常包含在互联网上暴露的金融应用 ,实际上攻击者是利用了例如跨站点脚本(XXS)、跨站点请求伪造 (CSRF) 以及 SQL 注入等软件漏洞，来访问信用卡信息等敏感数据。

83% 的受访者表示，在金融软件和系统中实施与网络安全相关的控制非常紧迫 (给出 7-10 分的受访者比例，10 分制，1= 不紧迫，10= 非常紧迫) 。只有 25% 的受访者有信心在产品发布前能够检测出金融软件和系统中的安全漏洞 (给出 7-10 分的受访者比例，10 分制，1= 毫无信心，10= 非常有信心) 。

图8. 对金融软件技术漏洞的担心

此处显示的是给出7-10分的受访者比例，计分从1到10， 1 = 毫不担心，10 = 非常担心

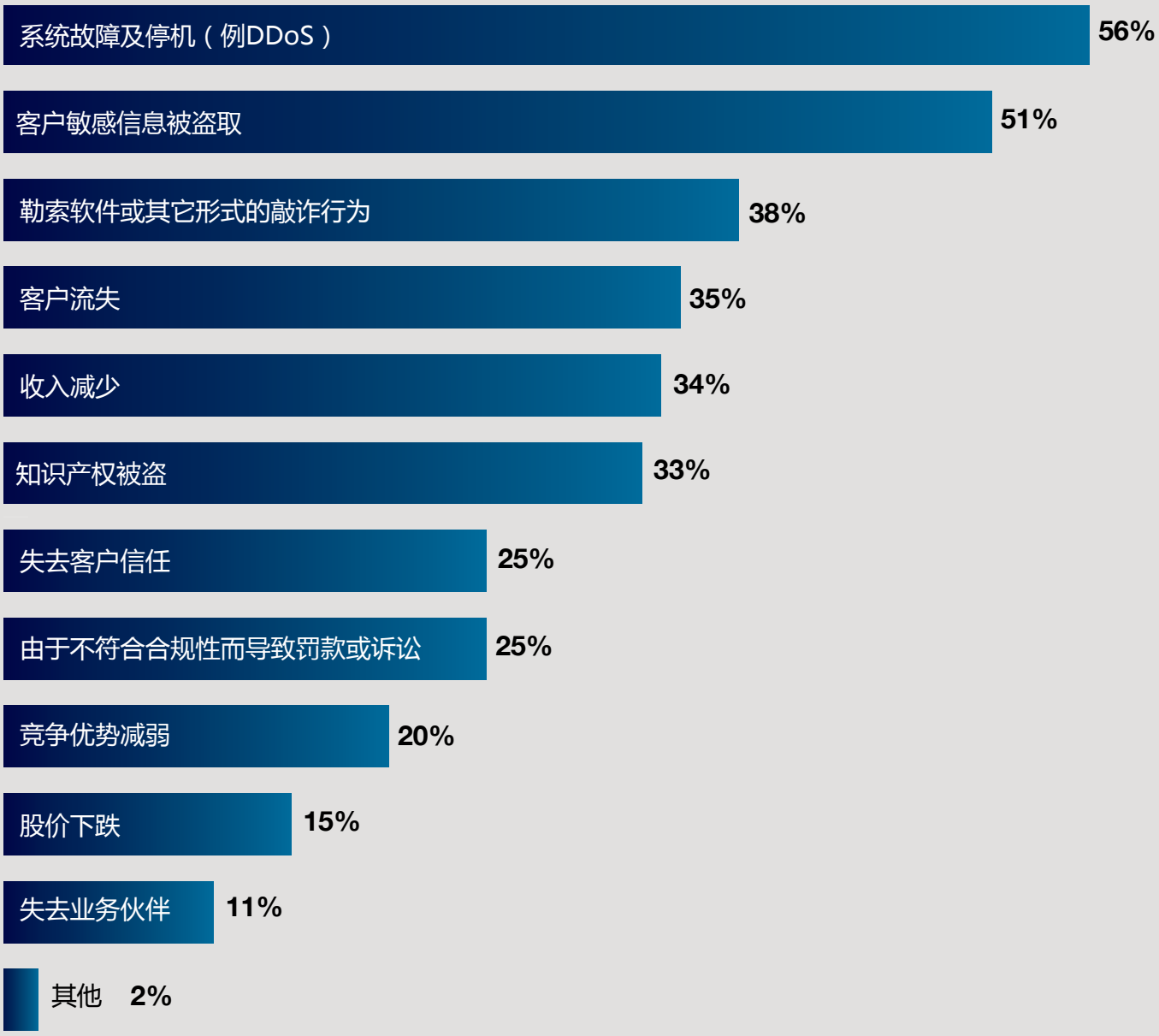


不安全的软件和技术对业务产生许多负面的影响，系统宕机是最频繁发生的。

图 9 显示了 11 种由不安全的金融服务软件和技术导致的负面业务影响。据 56%的受访者称，他们的机构遭遇过系统故障；超过一半（51%）表示客户的敏感信息被盗。

图 9. 贵机构是否曾遭遇由于不安全的金融服务软件和技术而导致负面的影响？

可多选



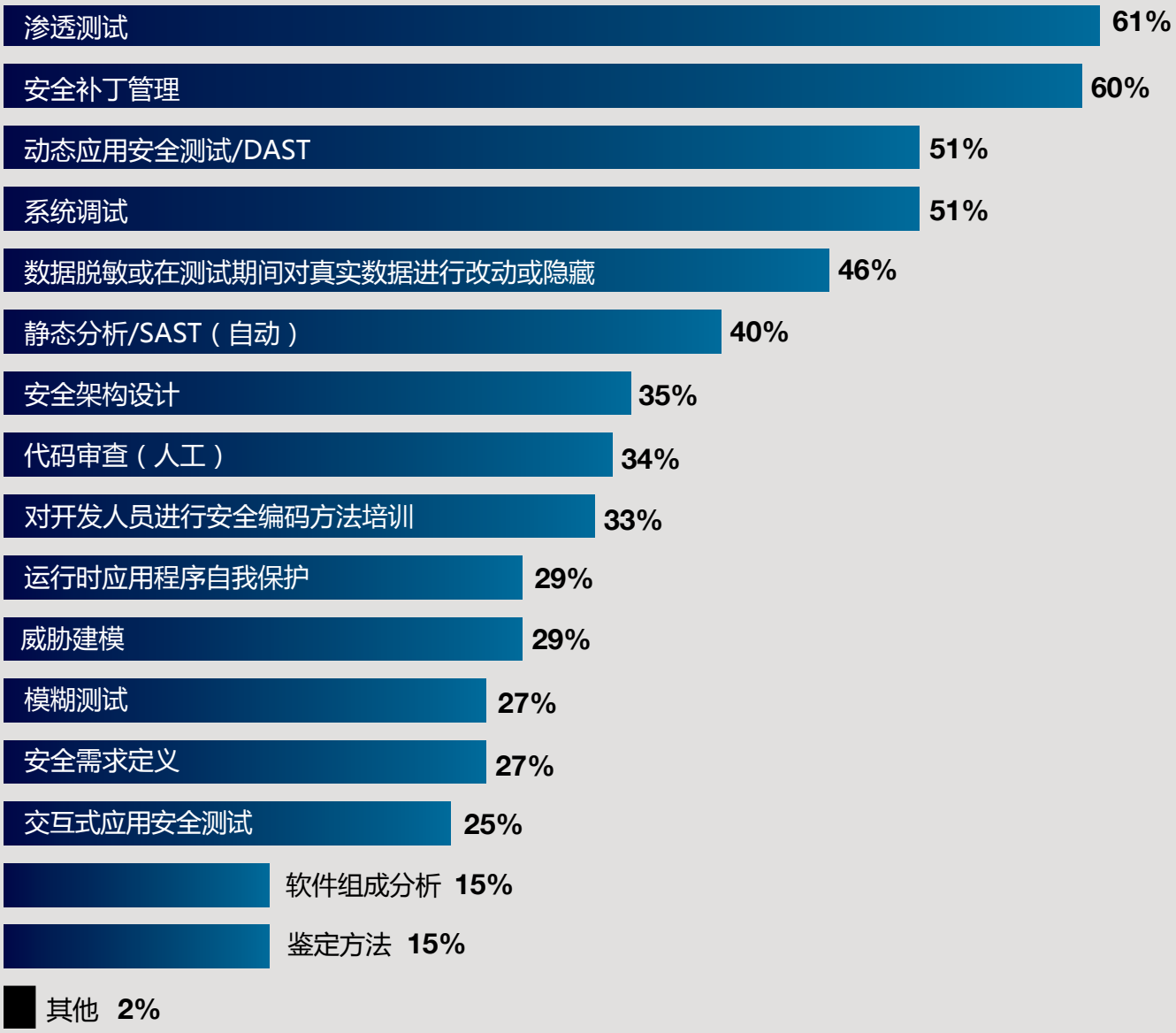
金融机构正在通过渗透测试和安全补丁管理来保护他们的金融软件和技术。

图 10 显示了金融机构为保护其金融软件和技术所做的 16 项活动。61% 受访者表示他们的机构进行渗透测试；60% 表示通过安全补丁修补安全漏洞。

一些机构还使用分层的方法，将自动化工具（如 SAST、SCA、IAST、DAST 和 RASP）与手工规划和测试活动（如安全架构设计、安全需求定义、威胁建模、代码评审和模糊测试等）相结合，以确保 SDLC 每个阶段的安全性。

图10. 贵机构如何确保金融软件和技术的安全性？

可多选



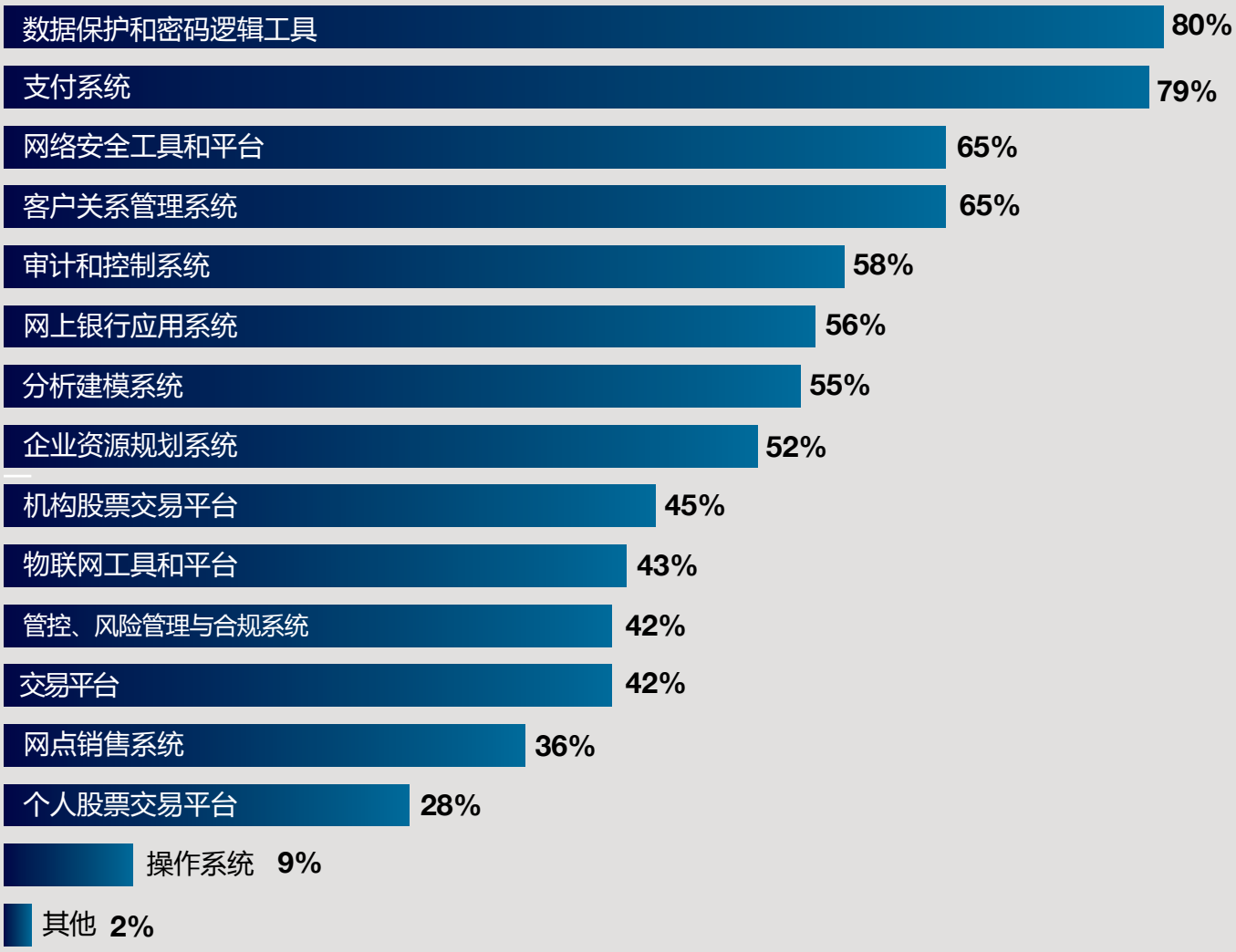
金融服务技术设计与开发的安全实践

金融服务公司设计并开发种类繁多的软件和技术。

图 11 显示了受访者指出其机构设计和开发的 15 种不同类型的金融服务软件和技术。80% 的受访者表示，他们设计并开发数据保护和密码逻辑工具，79% 的受访者表示，他们设计并开发支付系统。紧随其后的是网络安全工具和平台以及客户关系管理系统（均占 65%）。

图11. 贵机构设计和开发哪些类型的金融服务软件和技术？

可多选

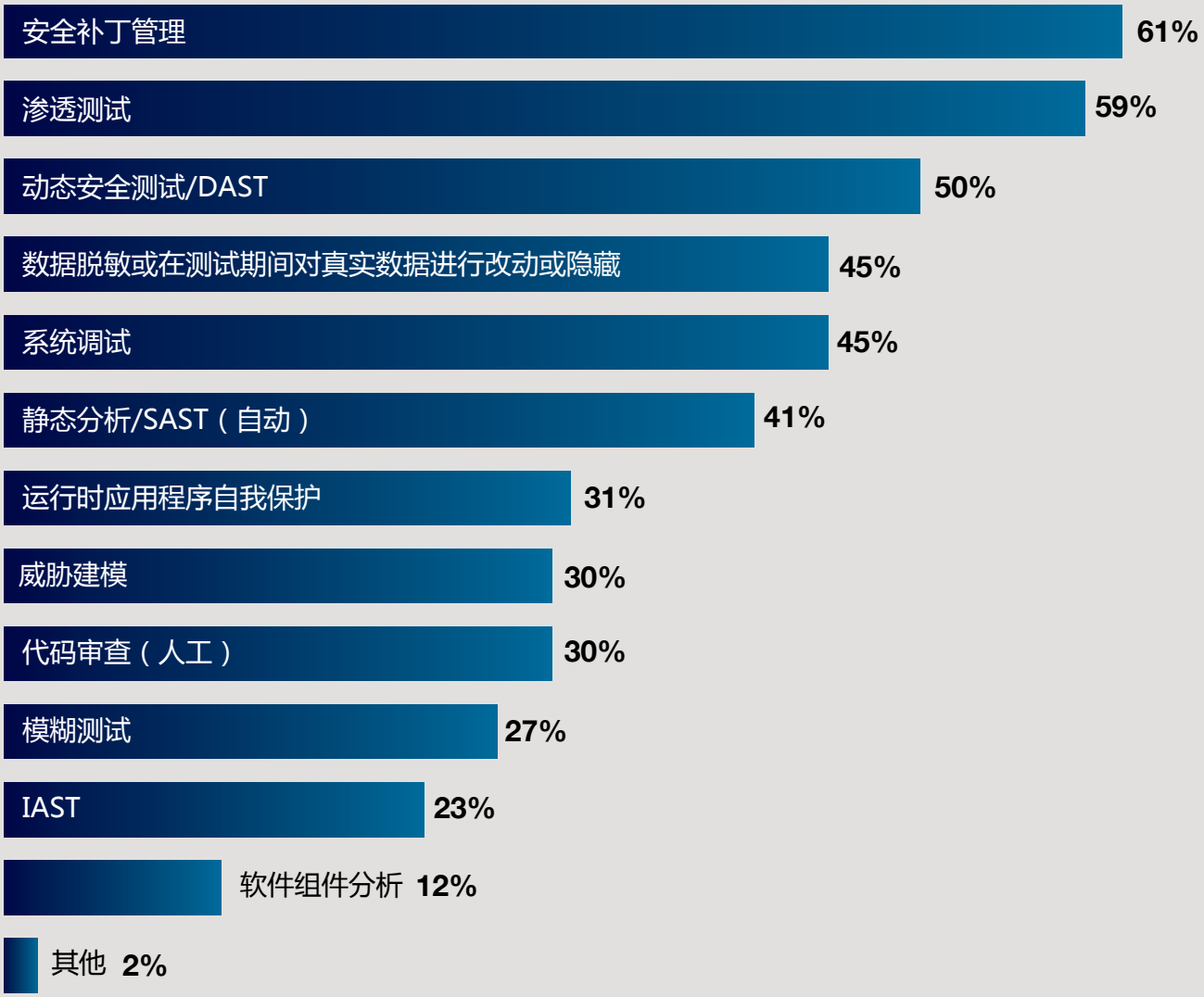


为保证质量，各机构纷纷依赖于安全补丁管理和渗透测试。

如图 12 所示，61% 的受访者表示他们的机构会修补漏洞，59% 的受访者表示他们会开展渗透测试，50% 的受访者表示他们会开展动态安全测试。

图12. 贵机构使用怎样的安全测试工具来保证质量？

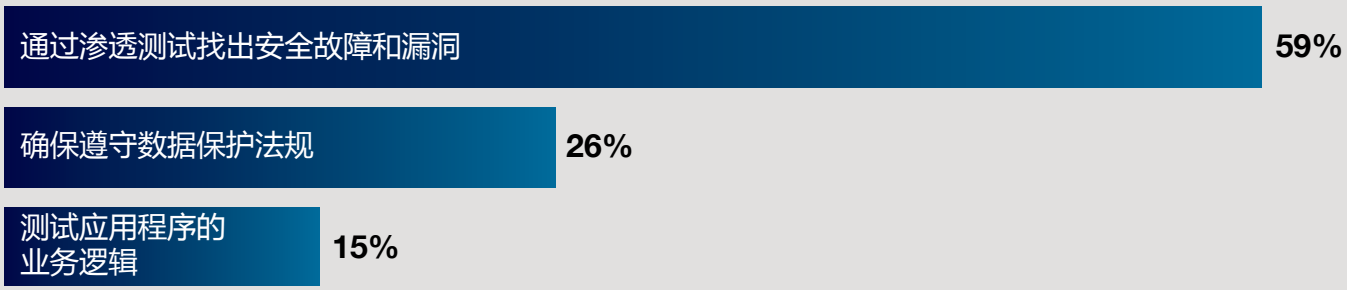
可多选



通过渗透测试来保证质量的机构受访者表示，他们开展渗透测试的主要原因（图 13）是通过测试找出安全故障和漏洞 (59%) 以及确保遵守数据保护法规 (26%)。只有 15% 的受访者表示其开展渗透测试是为了测试应用程序的业务逻辑。

图13. 为何要开展渗透测试？

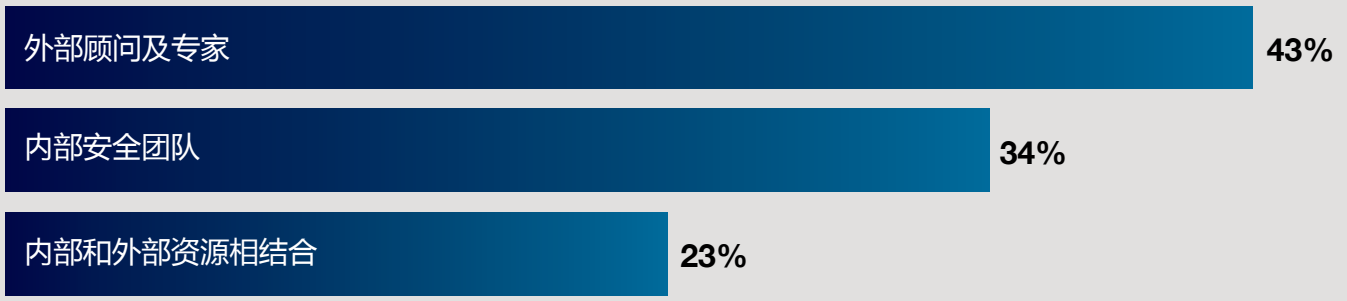
59%的受访者表示其机构开展渗透测试



实施威胁建模的机构受访者表示，这项任务通常由外部顾问和专家 (43%) 或内部安全团队 (34%) 执行，如图 14 所示。

图14. 贵机构如何实施威胁建模？

30%的受访者表示其机构实施威胁建模

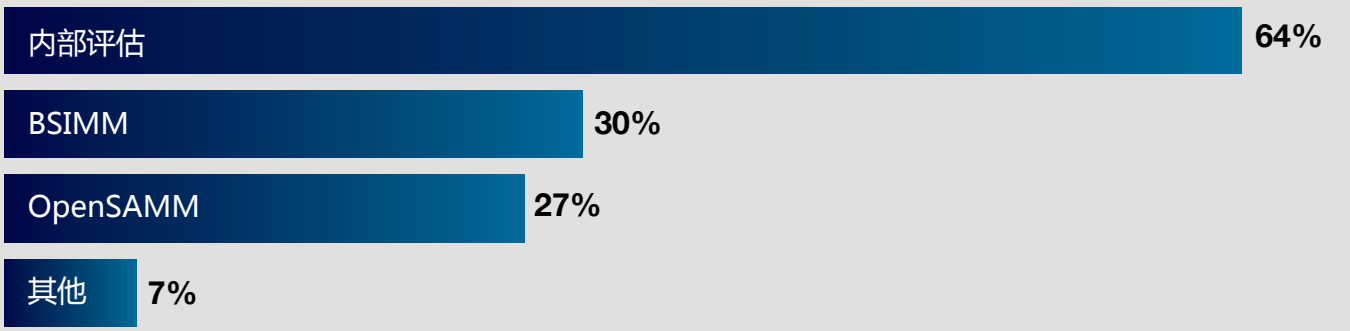


大多数机构通过开展内部评估来确定其安全现状的有效性。

如图 15 所示，64%的受访者表示他们的机构使用内部评估来评估安全现状。只有 30%的人表示他们使用 BSIMM，其次是 OpenSAMM (27%)。

图15. 贵机构应用哪种工具评估机构安全现状？

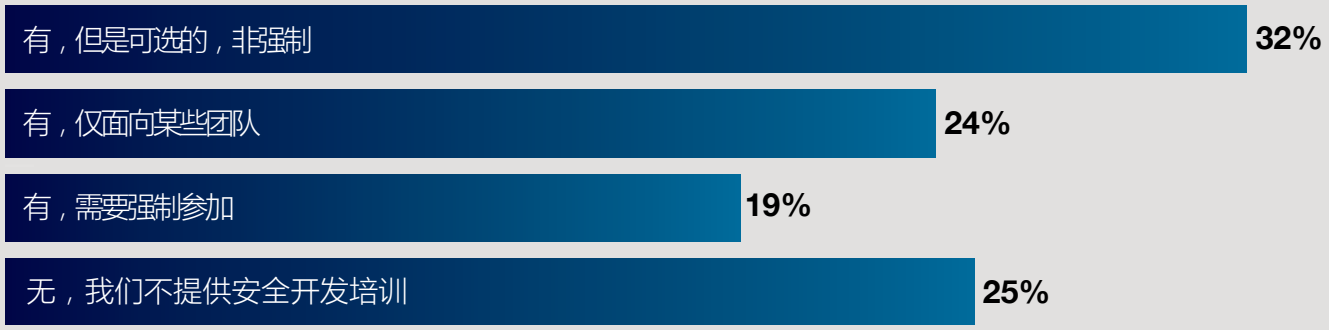
可多选



大多数机构为其软件开发人员提供安全开发培训，但只有 19% 的受访者表示这是一项强制性活动。

如图 16 所示，75%的机构提供一定程度的培训。但是，32%的受访者表示这是可选的；24%表示仅适用于某些团队；只有 19%表示培训需要强制参加。

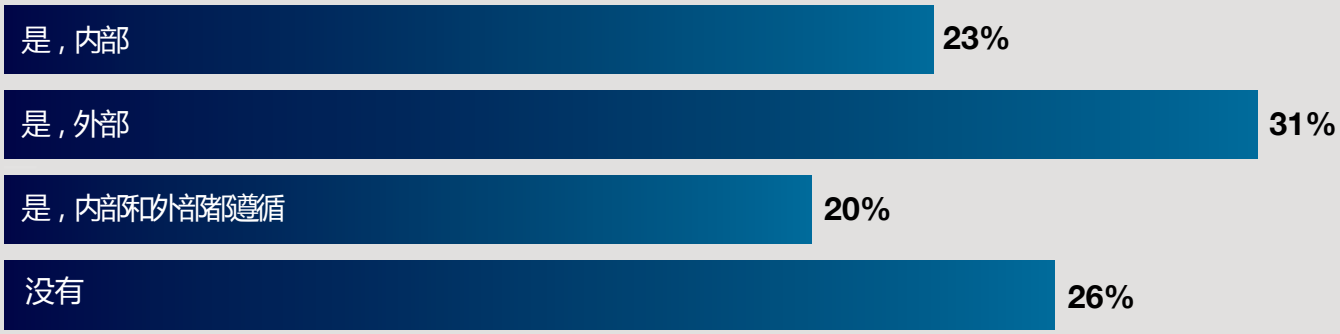
图16. 贵机构是否为软件开发人员提供安全开发培训？



大多数机构遵循已发布的安全软件开发生命周期 (SSDLC) 流程。

如图 17 所示，74%的受访者表示其机构内部（23%）、外部（31%） 或两者（20%）都遵循 SSDLC 流程。但是，平均而言，金融机构仅对 34% 的金融软件 / 技术进行网络安全漏洞测试。

图17. 贵机构是否遵循已发布的SSDLC？

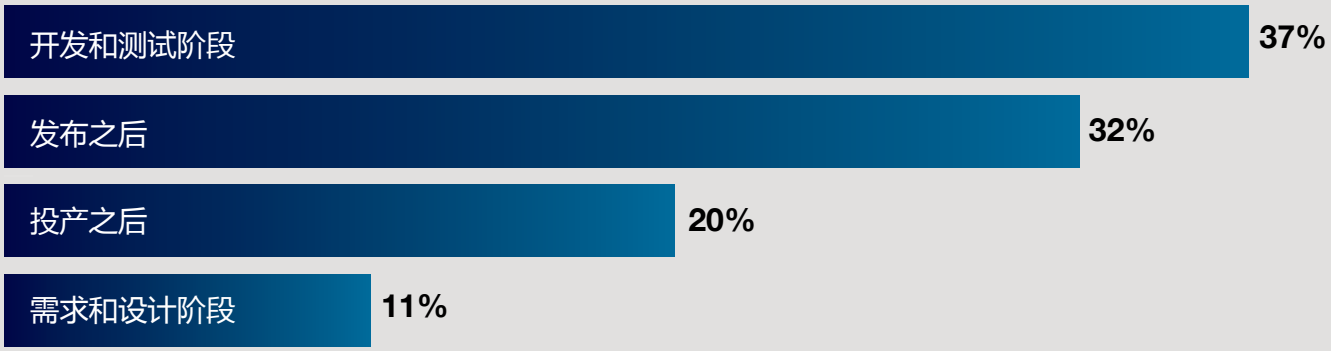


各机构通常只在软件发布之后才开展网络安全漏洞评估。

如图 18 所示，52% 的受访者表示网络安全漏洞评估发生在产品发布之后 (32%) 或产品投产之后 (20%)。不到一半 (48%) 的受访者表示，其机构会在软件设计 (11%) 或开发和测试阶段 (37%) 开展这项活动。

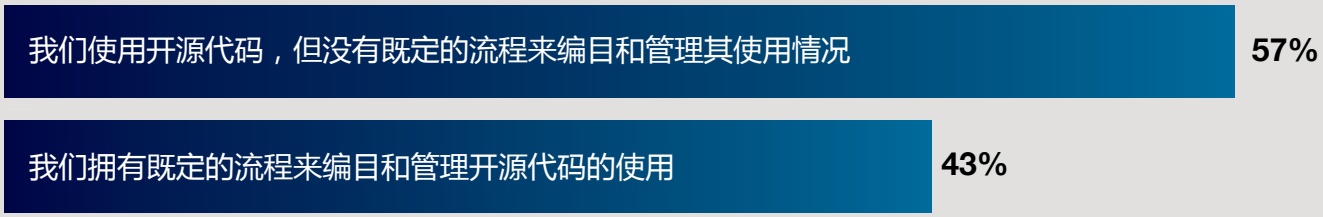
图18. 贵机构在软件开发生命周期的哪个阶段评估网络安全漏洞？

可多选



大多数机构都没有一个既定的流程来编目和管理其对开源代码的使用。只有 43% 的受访者表示，他们拥有既定的流程来编目和管理正在使用的源代码。

图19. 贵机构在使用开源代码开发金融软件和技术时有无标准可循？



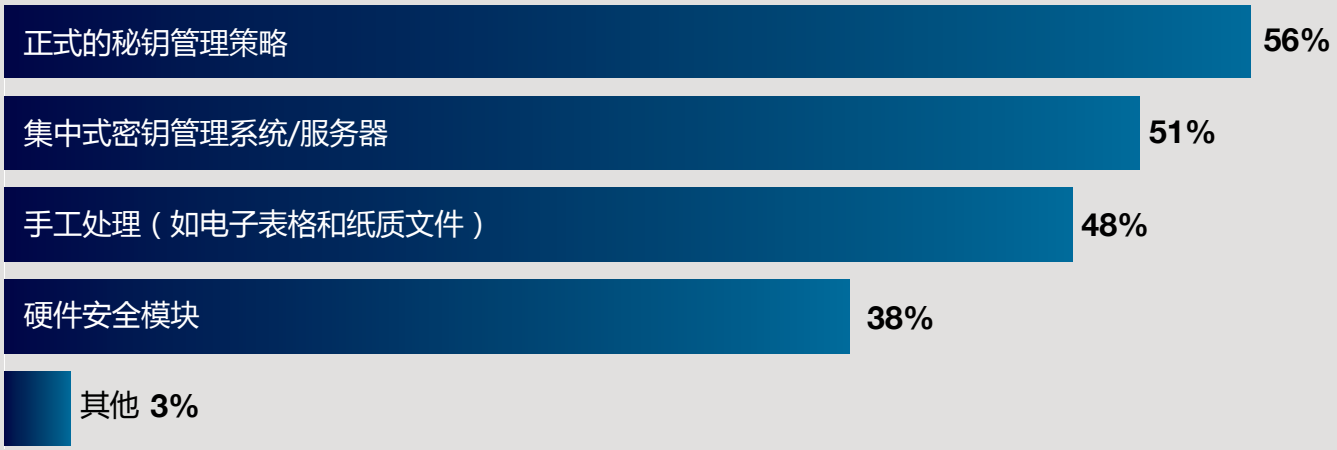
使用秘钥管理系统的机构通常拥有正式的秘钥管理策略。

近一半的机构 (48% 的受访者) 表示，他们使用关键管理系统来管理软件开发过程中使用的软件、技术和组件。他们使用的主要系统是正式的秘钥管理策略 (56%) 和集中式的秘钥管理系统或服务器 (51%)，如图 20 所示。

图20. 贵机构使用怎样的秘钥管理系统？

48%的受访者表示其机构使用秘钥管理系统

可多选



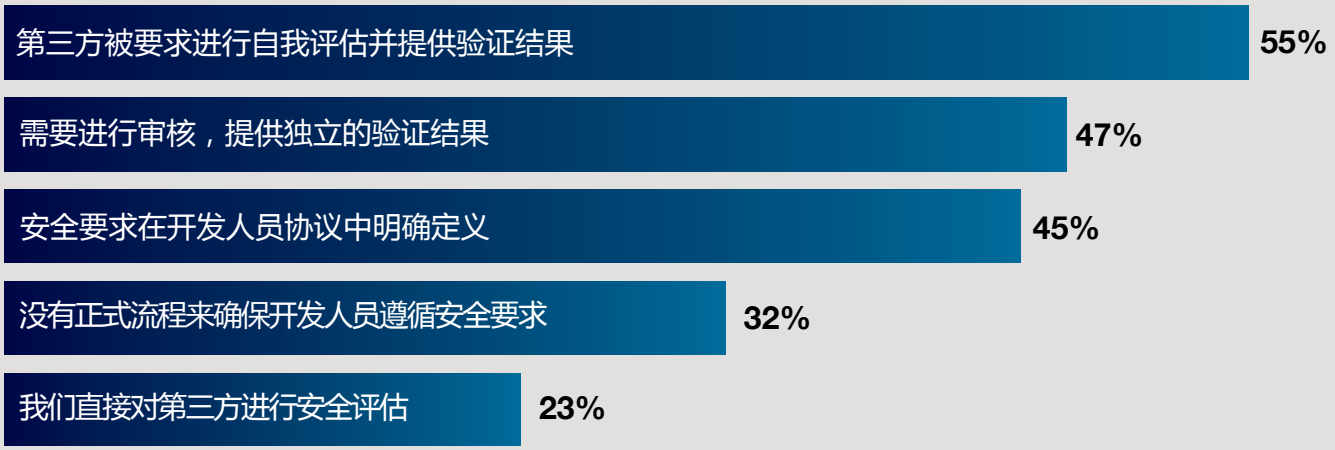
很多机构担心第三方风险，但大多数却不要求的第三方遵守他们的网络安全要求。

只有 43%的受访者表示他们要求参与金融软件技术开发过程的第三方验证其安全实践。如图 21 所示，55%要求第三方进行自我评估并提供验证结果。只有 23%直接对第三方进行安全评估。

图21. 贵机构如何确保第三方开发人员遵循安全要求？

43%的受访者表示其机构强制要求满足网络安全要求

可多选



结论和建议

风险和风险消减策略

鉴于许多 FSI 机构都依赖于第三方提供的软件，因此，对于参与本次调研的机构中只有不到一半要求第三方供应商遵守其软件安全实践这一结果，我们深表不安。

大多数的受访者指出，即使有这样的要求，他们的机构也会让第三方提供商自行开展验证和认证，而不是亲自进行检视。若要求供应商引入软件安全构建成熟度模型 (BSIMM) 等独立的外部成熟度模型，那么，金融机构将可以依据特定的机制来评估第三方软件供应商的安全成熟度。

软件代码中的 bug、缺陷和弱点很常见。FSI 机构可以通过使用（或要求第三方使用）自动 SAST（静态应用安全测试）工具来检测并报告可能生成安全漏洞的弱点，增强软件安全性，从而降低风险。

许多受访的 FSI 机构都没有建立开源代码的目录清单和管理流程。正如《2019 年度 Synopsys 开源安全与风险分析 (OSSRA) 报告》所指出的，Synopsys 黑鸭审计服务团队在 2018 年审查的超过 1,200 个代码库中，60% 至少包含一个开源漏洞。超过 40% 包含高危安全漏洞，68% 包含存在许可证冲突的组件。

使用开源软件的机构经常忽略相关的安全和许可风险。FSI 机构可能不会检视引入的第三方代码（或内部开发的代码），以发现潜在的安全和法律问题。FSI 若能通过全面的软件组成分析 (SCA) 解决方案来管理安全性、质量及许可合规风险，将能管控整个软件供应链和应用程序完整生命周期内开源代码带来的风险。

本次调研的受访者表示，系统故障和宕机是网络威胁造成最常见的业务影响。但更令人担忧的是，超过半数的受访者表示，他们所在机构的敏感客户信息曾一度被盗。

基于受访者经验，他们认为渗透测试和 DAST（动态应用安全测试）是降低网络安全风险最有效的活动。安全补丁管理、系统调试和威胁建模也非常有效。

然而，很显然，没有任何一种方法、工具或服务能够万无一失的保障软件安全性。一些机构使用自动化工具的分层方法，包括 SAST、SCA、IAST（交互式应用程序安全测试）、DAST 和 RASP（运行时应用程序安全测试）。而其他机构则采取人工规划和测试活动，如安全架构设计、安全需求定义、威胁建模、代码审查和模糊测试等，以确保 SDLC 每个阶段的安全性。

参与本次调研的受访者一致认为，云迁移工具以及紧随其后的区块链工具，是目前给 FSI 机构带来最大网络安全风险的技术。

虽然区块链技术的应用起步慢，但速度正在加快，类似于 10 年前云技术的应用。与云技术一样，区块链也存在不为人知的安全隐患，但 FSI 对其的使用很可能与 SWIFT（环球银行金融电信协会）系统类似。SWIFT 是消息传递网络，金融机构通过标准的系统代码来安全地传输信息和指令。

但是，区块链平台仍然容易受到来自外围网络基础设施、未经授权用户和内部威胁的入侵，从破坏区块链凭证并暴露敏感数据。随着基于区块链的网络不断发展，机构的离场和加入，数据共享、所有权、以及具有监管合规意义的数据治理多方面，很可能会存在歧义。

利用托管服务来补充内部资源

大多数受访者都希望借助更多的资源和内部专业知识来消减风险。鉴于许多团队 — IT 安全或其他团队 — 都认为他们的预算总不够用，因此，缓解资源紧缺问题的策略之一便是外包安全测试。与构建内部专门团队相比，将任务外包给提供渗透测试和 DAST 等服务的专业机构通常更省钱。

虽然调查结果显示，大多数的 FSI 机构都给软件开发人员提供安全开发培训，但只有极少一部分受访者 (19%) 表示这种培训是强制性的。强制要求产品开发人员参加网络安全技能培训可以帮助缓这一问题。产品开发团队中的安全冠军团队可以帮助宣传最佳安全实践，并支持其他团队成员解决和修复代码漏洞。

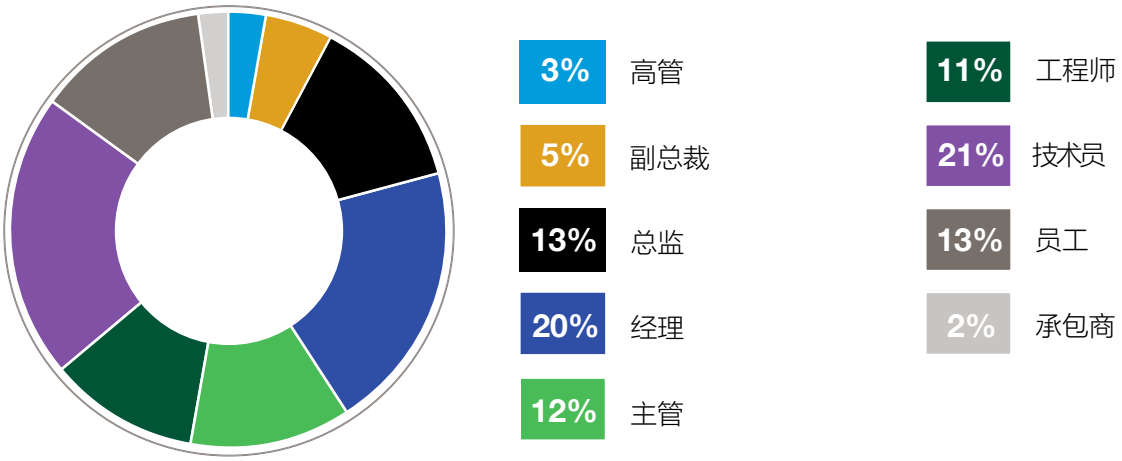
其他策略还包括：(1) 为开发团队提供具有上下文学习功能，并针对如何修复漏洞提供详细建议的 SAST 工具；(2) 定期提供由导师指导的代码开发安全培训会议。

方法

样本框架由来自金融服务行业各个领域的 1.145 万名 IT 和 IT 安全从业人员组成。如表 1 所示，共有 463 名受访者对调研进行了回复。除去剔除掉的 49 人，最终的样本是 414 人，最终的回复率是 3.6%。

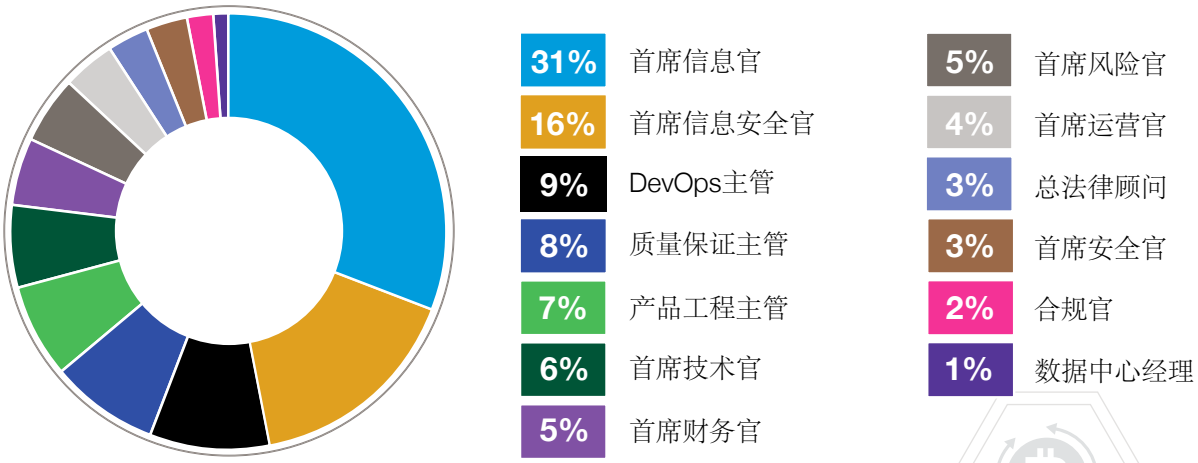
表 1. 样本回复情况	**频率**	**%**
• 总体样本框架	11,450	100.0%
• 做出回复的样本总数	463	4.0%
• 剔除掉的样本	49	0.4%
• 最终参与调研的样本	414	3.6%

饼图 1 显示了受访者目前的职位或组织级别。超过一半的受访者 (53%) 表示他们目前的职位是主管或以上。34% 的受访者表示他们目前的职位是技术员或普通员工。



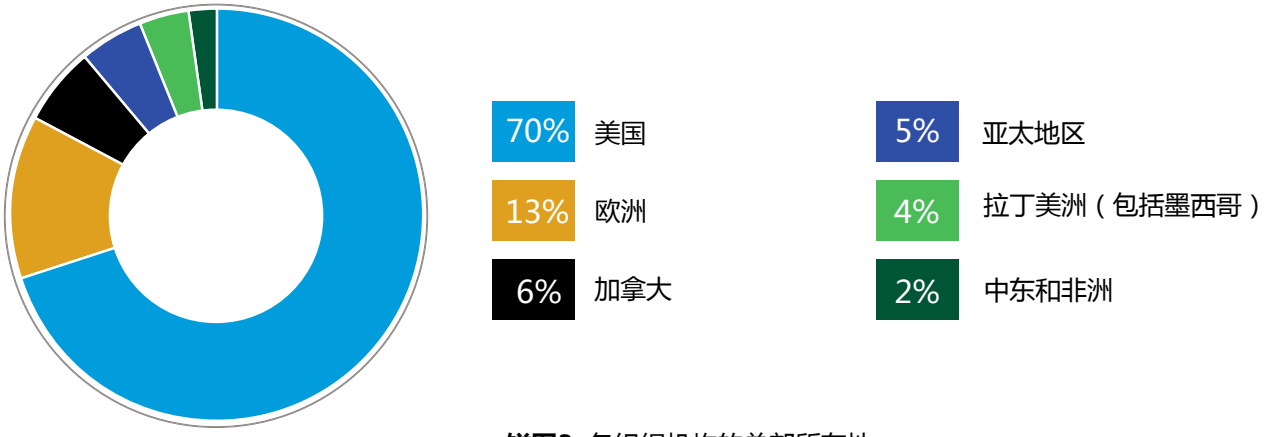
饼图1. 受访者目前的职位或组织级别

如饼图 2 所示，31% 的受访者表示他们的直接主管是首席信息官，16% 的直接主管是首席信息安全官，9% 的直接主管是 DevOps 负责人，8% 的直接主管质量保证负责人。



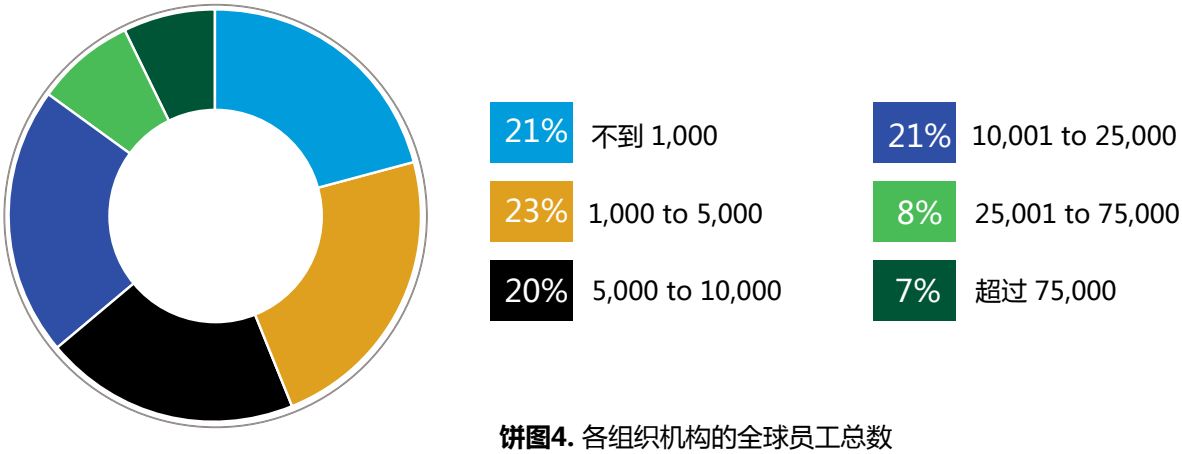
饼图2. 受访者的直接经理

70% 的受访者来自总部位于美国的机构，如饼图 3 所示。13% 来自总部设在欧洲的机构，其次是加拿大 (6%)、亚太地区 (5%)、拉丁美洲 (4%)、中东和非洲 (2%)。



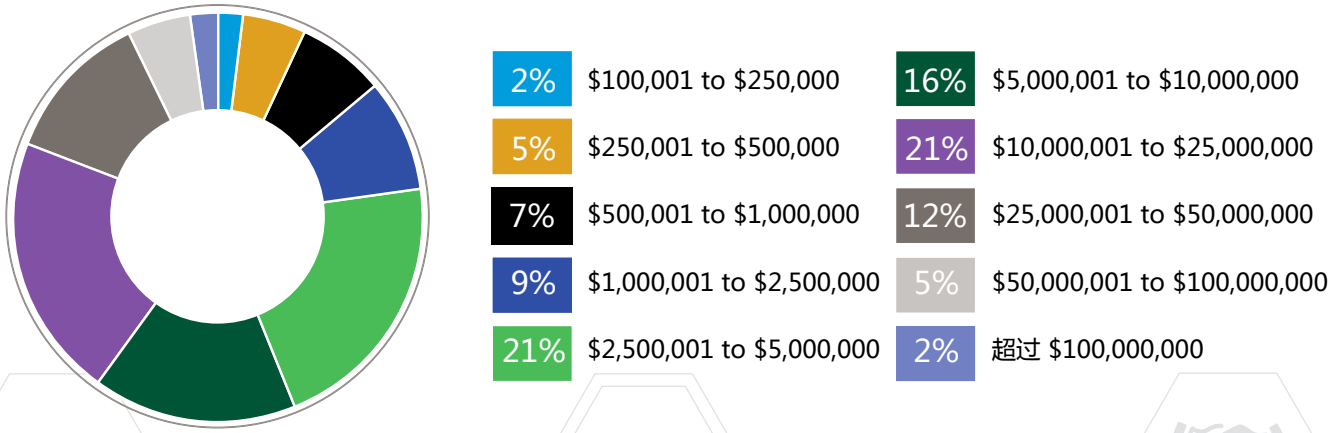
饼图3. 各组织机构的总部所在地

如饼图 4 所示，超过一半的受访者 (56%) 来自全球雇员超过 5,000 人的机构。



饼图4. 各组织机构的全球员工总数

如饼图 5 所示，超过一半的受访者 (58%) 在网络安全上的花费在 250 万美元到 2,500 万美元之间，其中包括技术、人员、管理或外包服务以及其他相关现金支出等领域的总投资。

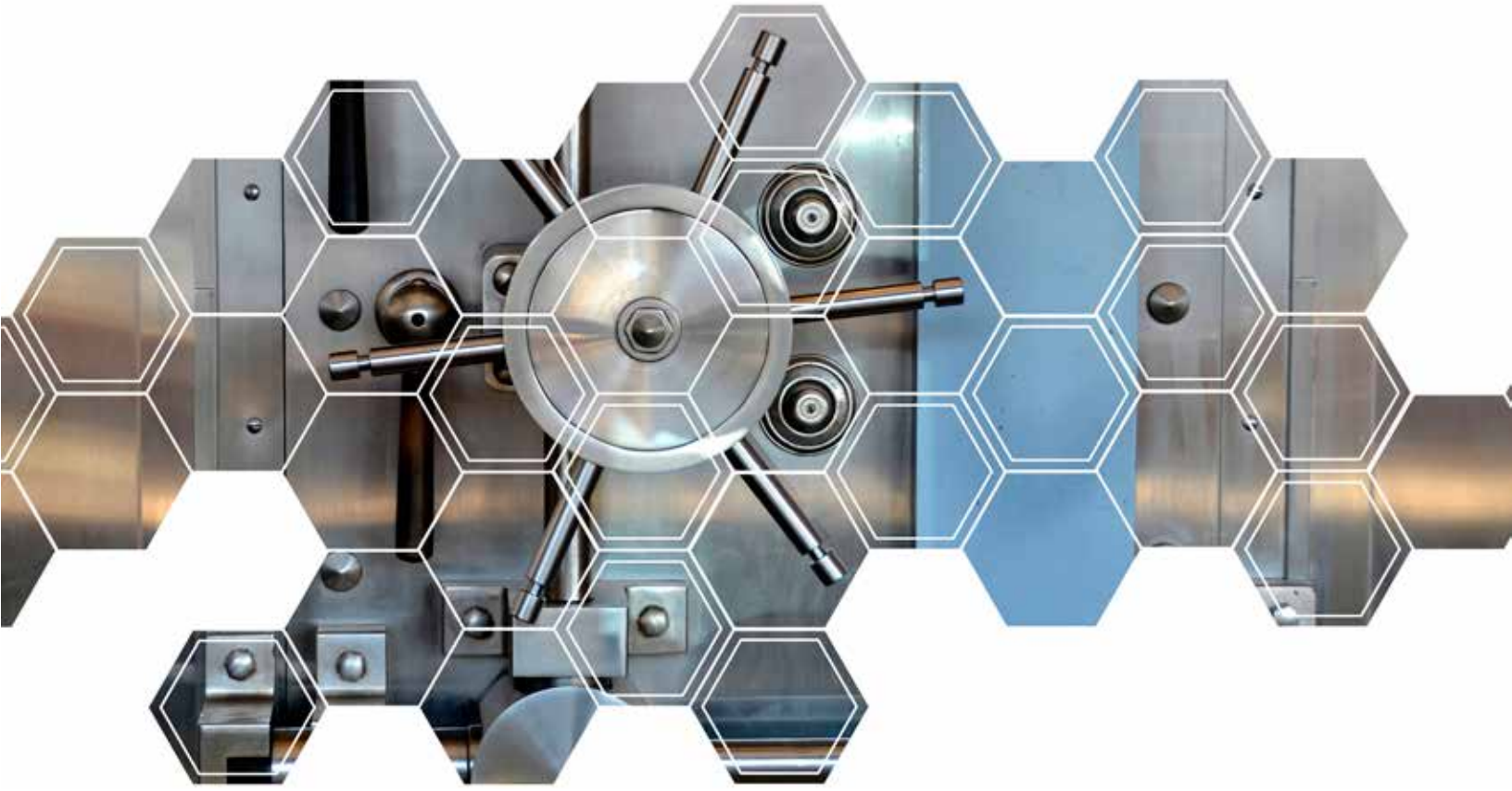


饼图5. 基于网络安全支出的受访者分布

关于本次调研的几点注意事项

得出结论之前，需要仔细考虑调查研究的固有局限性。以下各项是与大多数在线调研相关的特定限制。

- 无反应偏差：目前的调研结果基于调研样本的反馈。我们针对金融服务业所有领域的 IT 和 IT 安全从业人员的代表性样本开展了调研，并收到了大量有用的反馈。尽管开展了无反应测试，但没有参加测试的人员与完成测试的人员在潜在信念方面总是有很大的不同。
- 抽样框架偏差：准确性取决于联系信息以及名单中的人员能从多大程度上代表不同机构的 IT 人员和 IT 安全从业人员。因为我们采用了在线调研方法，因此，邮件或电话等非在线形式的回复可能会导致调研结果产生出入。
- 自我报告结果：调研的质量取决于受访者的诚信度。虽然在调研过程中可以纳入某些制衡手段，但仍然不排除被调研对象没有提供准确答复的可能性。



附录：具体调研结果

下表显示了本次调研中所有调查问题的回复频率或百分比频率 (Pct%)，是 2019 年 1 月 12 日至 2 月 9 日期间收集到的所有调查回复。

样本回复情况	频率	%
• 总体样本框架	11,450	100.00%
• 做出回复的样本总数	463	4.04%
• 剔除掉的样本	49	0.43%
• 最终参与调研的样本	414	3.62%

第 1 部分 . 筛选

S1a. 您是否参与贵机构金融应用的安全评估工作？	• 是，经常参与	44%
	• 是，偶尔参与	40%
	• 是，极少参与	16%
	• 否，不参与（剔除）Stop)	0%
	总计	100%
S1b. 如果您参与其中，您参与评估应用程序的安全性工作几年了？	• 不到 1 年	2%
	• 2-4 年	15%
	• 5-7 年	28%
	• 8-10 年	30%
	• 超过 10 年	25%
	• 无法决定（剔除）	0%
	总计	100%
	推断值	7.85
S2. 哪一项描述您所在的组织在金融应用程序开发中扮演的角色最为恰当？	• 开发和构建金融应用	27%
	• 安装和实施金融应用	45%
	• 为金融服务业提供服务	23%
	• 其他 (请注明)	5%
	• 以上皆非 (剔除)	0%
	总计	100%
S3. 哪一项描述在金融应用开发中扮演的角色最为恰当？	• 银行	40%
	• 保险	19%
	• 经纪	12%
	• 投资管理	7%
	• 支付处理	5%
	• 按揭贷款 / 处理	15%
	• 其他 (请注明)	2%
	• 以上皆非 (剔除)	0%
	总计	100%

第 2 部分 一般性问题

Q1. 以 10 分制计，请评估贵机构在预防网络攻击方面的有效性。1 = 无效，10 = 非常有效。	• 1 到 2	11%
	• 3 到 4	24%
	• 5 到 6	34%
	• 7 到 8	16%
	• 9 到 10	15%
	总计	100%
	推断值	5.50

Q2. 以 10 分制计，请评估贵机构在检测网络攻击方面的有效性。1 = 无效，10 = 非常有效。	• 1 到 2	5%
	• 3 到 4	10%
	• 5 到 6	29%
	• 7 到 8	35%
	• 9 到 10	21%
	总计	100%
	推断值	6.64

Q3. 以 10 分制计，请评估贵机构在控制网络攻击方面的有效性。1 = 无效，10 = 非常有效。	• 1 到 2	8%
	• 3 到 4	11%
	• 5 到 6	28%
	• 7 到 8	28%
	• 9 到 10	25%
	总计	100%
	推断值	6.52

Q4. 贵机构设计和开发了哪些类型的金融服务软件 / 技术？请选择所有的适用项。	• 企业资源规划 (ERP) 系统	52%
	• 在线银行应用	
	• 交易平台	56%
	• 交易平台	42%
	• 个人股票交易平台	28%
	• 机构股票交易平台	45%
	• 客户关系管理 (CRM) 系统	65%
	• 支付系统	79%
	• 物联网 (IoT) 工具和平台	43%
	• 网点系统	36%
	• 管控、风险管理与合规 (GRC) 系统	42%
	• 分析建模系统	55%
	• 审计和控制系统	58%
	• 网络安全工具和平台	65%
	• 数据保护和密码逻辑工具	80%
	• 操作系统	9%
	• 其他 (请注明)	2%
	总计	757%

Q5a. 贵机构有无网络安全项目或团队？	• 有	67%
	• 无	33%
	总计	100%
Q5b. 如果有，贵机构的保障网络安全的方法是什么？	• 网络安全是传统 IT 网络安全团队的一部分，是 IT 网络安全团队的职责之一（通常在全球 CISO 的领导下）	60%
	• 确保网络安全是功能性安全团队的职责之一	34%
	• 网络安全团队是集中的（即卓越中心），指导并支持 47% 多个产品开发团队	47%
	• 网络安全团队是分散的，网络安全专家隶属于特定 51% 的产品开发团队	51%
	• 确保网络安全是产品开发团队的职责之一	23%
	• 其他（请注明）	3%
	总计	218%
Q6. 我的机构为确保网络安全分配了足够的资源（即预算及人力）。	• 强烈同意	15%
	• 同意	30%
	• 不确定	17%
	• 不同意	31%
	• 极不同意	7%
	总计	100%
Q7. 我的机构在产品开发方面具备必要的网络安全技能。	• 强烈同意	12%
	• 同意	26%
	• 不确定	18%
	• 不同意	32%
	• 极不同意	12%
	总计	100%

第 3 部分 对软件安全风险的认识

Q8. 哪些软件 / 技术对金融服务公司的网络安全风险最大？请选择最适用的五 (5) 项。	• 企业资源规划 (ERP) 系统	10%
	• 客户关系管理 (CRM) 系统	38%
	• 支付系统	50%
	• 网点销售系统	45%
	• 区块链工具	52%
	• 物联网 (IoT) 工具和平台	48%
	• 管控、风险管理与合规 (GRC) 系统	21%
	• 分析建模系统	50%
	• 审计和控制系统	16%
	• 网络安全工具和平台	28%
	• 数据保护和密码逻辑工具	35%
	• 云迁移工具	60%
	• 操作系统	45%
	• 其他（请注明）	2%
	总计	500%

Q9. 贵机构开发或使用的不安全的金融服务软件 / 技术，会对业务造成下列哪项负面影响？请选择所有的适用项。	• 客户敏感信息被盗	51%
	• 知识产权被盗	33%
	• 系统故障和停机 (例如 DDoS)	56%
	• 勒索软件和其他 (请注明) 形式的敲诈勒索	38%
	• 合规失败导致的罚款或诉讼	25%
	• 收入损失	34%
	• 客户流失	35%
	• 商业伙伴流失	11%
	• 失去客户的信任	25%
	• 股价下跌	15%
	• 丧失竞争优势	20%
	• 其他 (请注明)	2%
	总计	345%

Q10. 您是否知道贵机构因不安全的金融软件而导致用户身份凭证　被盗取？	• 是	23%
	• 否	77%
	总计	100%

请以 10 分制对下列陈述进行评分，1 = 毫不担心，10 = 非常担心。

Q11. 您对贵机构所开发的金融软件 / 系统的网络安全状况有多担心？	1 或 2	5%
	• 3 或 4	8%
	• 5 或 6	25%
	• 7 或 8	27%
	• 9 或 10	35%
	总计	100%
	推断值	7.08

Q12. 您对第三方为贵机构提供的金融软件 / 系统的网络安全状况有多担心？	• 1 或 2	3%
	• 3 或 4	7%
	• 5 或 6	16%
	• 7 或 8	32%
	• 9 或 10	42%
	总计	100%
	推断值	7.56

Q13. 您对整个金融服务行业的网络安全有多担心？	• 1 或 2	7%
	• 3 或 4	5%
	• 5 或 6	23%
	• 7 或 8	35%
	• 9 或 10	30%
	总计	100%
	推断值	7.02
Q14. 您对贵机构的网络安全实践跟不上金融服务技术的变化步伐有多担心？	• 1 或 2	8%
	• 3 或 4	10%
	• 5 或 6	31%
	• 7 或 8	25%
	• 9 或 10	26%
	总计	100%
	推断值	6.52
Q15. 您对金融服务行业的网络安全监管要求跟不上金融技术的变化步伐有多担心？	• 1 或 2	2%
	• 3 或 4	9%
	• 5 或 6	32%
	• 7 或 8	29%
	• 9 或 10	32%
	总计	104%
	推断值	7.32
Q16. 您对金融服务行业的网络安全监管要求太难遵守有多担心？	• 1 或 2	10%
	• 3 或 4	14%
	• 5 或 6	32%
	• 7 或 8	29%
	• 9 或 10	15%
	总计	100%
	推断值	6.00
Q17. 您对贵机构开发或使用金融软件 / 技术成为恶意行为人的目标有多担心？	• 1 或 2	2%
	• 3 或 4	6%
	• 5 或 6	8%
	• 7 或 8	30%
	• 9 或 10	54%
	总计	100%
	推断值	8.06

请以 10 分制对下列陈述进行评分，1 = 毫无信心，10 = 非常有信心。		
Q18. 您对金融软件 / 系统的安全漏洞在上市前可以被检测出来拥有几成信心？	• 1 或 2	13%
	• 3 或 4	27%
	• 5 或 6	35%
	• 7 或 8	13%
	• 9 或 10	12%
	总计	100%
	推断值	5.18

请以 10 分制对下列陈述进行评分，1 = 毫不困难，10 = 非常困难。		
Q19. 对贵机构而言，在进入市场之前检测出汽车软件 / 技术 / 组件中的安全漏洞有多困难？	• 1 或 2	1%
	• 3 或 4	8%
	• 5 或 6	15%
	• 7 或 8	33%
	• 9 或 10	43%
	总计	100%
	推断值	7.68

请以 10 分制对下列陈述进行评分，1 = 毫不紧迫，10 = 非常紧迫。		
Q20. 在金融软件 / 系统中实施与网络安全相关的控制对贵机构而言有多紧迫？	• 1 或 2	3%
	• 3 或 4	5%
	• 5 或 6	9%
	• 7 或 8	37%
	• 9 或 10	46%
	总计	100%
	推断值	7.86

第 4 部分 SDLC 安全实践

Q21a. 贵机构是否为软件开发人员提供安全开发培训？	• 是，可选的	32%
	• 是，强制性的	19%
	• 是，只针对特定团队	24%
	• 否，我们不提供安全开发培训	25%
	总计	100%
Q21b. 如果是，贵机构安全开发培训的效果如何？	• 非常有效	17%
	• 有效	21%
	• 一般	28%
	• 无效	34%
	总计	100%

Q22. 贵机构在创建金融软件 / 技术时是否遵循内部或外部发布的安全软件开发生命周期 (SSDLC) 流程？	• 是，遵循内部流程	23%
	• 是，遵循外部流程	31%
	• 是，同时遵循内外部流程	20%
	• 否	26%
	总计	100%
Q23. 平均而言，在贵机构开发或使用的金融软件 / 技术中，经过网络安全漏洞测试的比例是多少？	• 无	12%
	• 不到 25%	25%
	• 26%-50%	43%
	• 51%-75%	12%
	• 76%-100%	8%
	总计	100%
	推断值	34%
Q24. 在软件开发生命周期中，贵机构在哪个阶段评估网络安全漏洞？请选择所有的适用项。	• 需求和设计阶段	11%
	• 开发和测试阶段	37%
	• 发布后	32%
	• 投产后	20%
	总计	100%
Q25. 贵机构采取哪些的活动来确保金融软件 / 技术的安全？请选择所有的适用项。	• 培训开发人员安全编码方法	33%
	• 安全架构设计	35%
	• 威胁建模	29%
	• 识别方法	15%
	• 安全需求定义	27%
	• 代码审查 (人工)	34%
	• 静态分析 /SAST(自动化)	40%
	• 系统调试	51%
	• 模糊测试	27%
	• 软件组成分析	15%
	• 动态安全测试 /DAST	51%
	• 交互式应用程序安全性测试 (IAST)	25%
	• 渗透测试	61%
	• 数据脱敏或在测试期间对真实数据进行改动或隐匿	46%
	• 安全补丁管理	60%
	• 运行时应用程序自我保护 (RASP)	29%
	• 其他 (请注明)	2%
	总计	580%

Q26. 在降低金融服务行业的网络安全风险方面，哪些活动是最有效的？请选择所有的适用项。	• 培训开发人员安全编码方法	44%
	• 安全架构设计	25%
	• 威胁建模	51%
	• 识别方法	23%
	• 安全需求定义	34%
	• 代码审查 (人工)	40%
	• 静态分析 /SAST(自动)	45%
	• 系统调试	52%
	• 模糊测试	49%
	• 软件组成分析	33%
	• 动态安全测试 /DAST	63%
	• 交互式应用程序安全性测试 (IAST)	28%
	• 渗透测试	65%
	• 数据脱敏或在测试期间对真实数据进行改动或隐匿	43%
	• 安全补丁管理	55%
	• 运行时应用程序自我保护 (RASP)	23%
	• 其他 (请注明)	0%
	总计	673%
Q27. 贵机构在使用开源代码开发金融软件和技术时有无标准可循	• 我们有既定的流程来编录和管理开源代码的使用。	43%
	• 我们使用开源代码，但没有既定的流程来编录和管理其使用。	57%
	总计	100%
Q28. 贵机构是否拥有补丁管理流程（例如：明确角色和职责，并且补丁处理流程建立了指导指南）？	• 有	51%
	• 无	49%
	总计	100%
Q29a. 贵机构是否针对开发或制造过程中使用的软件 / 技术 / 组件使用秘钥管理系统？	• 是	48%
	• 否	52%
	总计	100%

Q29b. 如果是，贵机构目前使用怎样的秘钥管理系统？请选择所有的适用项。	• 正规的秘钥管理策略 (KMP)	56%
	• 手工流程 (如电子表格和纸质流程)	48%
	• 集中秘钥管理系统 / 服务器	51%
	• 硬件安全模块	38%
	• 其他 (请注明)	3%
	总计	196%
Q30a. 贵机构是否针对参与金融软件 / 技术开发流程的承包商、业务伙伴和其他 (请注明) 第三方提出了强制性的网络安全要求？	• 是	43%
	• 否	57%
	总计	100%
Q30b. 如果是，贵机构是如何第三方开发人员遵循安全相关要求？请选择所有适用项。	• 要求第三方进行自我评估，并提供认证和验证	55%
	• 需要开展独立审计，以提供认证和验证	47%
	• 我们直接对第三方进行安全评估	23%
	• 在开发人员协议中明确定义安全要求	45%
	• 我们没有正式的流程来确保开发人员遵守安全要求	32%
	总计	202%

第 5 部分 技术趋势

Q31. 贵机构是否采用了诸如 DevOps 和 CI/CD 之类的快速开发方法？	• 是	35%
	• 否，但我们计划明年开始	23%
	• 否，但我们计划在未来 24 个月内开始	12%
	• 我们没有采用这些方法的计划	30%
	总计	100%
Q32. 如果是，您是否已将安全性融入到了 DevOps 及 / 或 CI/CD 工作流中？	• 是	50%
	• 否，但我们计划明年开始	16%
	• 否，但我们计划在未来 24 个月内开始	11%
	• 我们没有采取安全措施的计划	23%
	总计	100%
Q33. 您对纽约金融服务局 (NYDFS) 面向金融服务公司的规定有多熟悉？	• 非常熟悉	27%
	• 熟悉	44%
	• 不熟悉 (跳至 Q36a)	23%
	• 没概念 (跳至 Q36a)	6%
	总计	100%

Q34a. 贵机构是否符合 NYDFS 的规定？	• 是的，完全符合	20%
	• 是的，部分符合	32%
	• 否，但我们将在今年实现合规	25%
	• 否，我们不确定何时能实现合规	23%
	总计	100%
Q34b. 如果是，贵机构实现合规的难度有多大？以 10 分计，1 = 毫无困难，10 = 非常困难。	• 1 到 2	2%
	• 3 到 4	5%
	• 5 到 6	10%
	• 7 到 8	50%
	• 9 到 10	33%
	总计	100%
	推断值	7.64
Q35. 在您看来，遵守 NYDFS 网络安全法规对贵机构的整体网络安全态势的效果有何影响？	• 非常显著的改善	21%
	• 显著改善	30%
	• 几乎没有改善	29%
	• 没有改善	20%
	总计	100%
Q36a. 贵机构是否需要遵守欧盟于 2018 年 5 月 25 日颁布实施的《通用数据保护条例》(GDPR)?	• 是	64%
	• 否 (跳至 Q39a)	36%
	总计	100%
Q36b. 如果是，贵机构是否符合 GDPR 的规定？	• 是的，完全符合	27%
	• 是的，部分符合	54%
	• 我们迄今为止尚未做到符合规定 (跳至 Q39a)	19%
	总计	100%
Q37. 对贵机构而言，实现 GDPR 合规的难度有多大？以 10 分计，1 = 毫无困难，10 = 非常困难。	• 1 到 2	0%
	• 3 到 4	3%
	• 5 到 6	8%
	• 7 到 8	52%
	• 9 到 10	37%
	总计	100%
	推断值	7.96

Q38. 在您看来，遵守 GDPR 对贵机构的整体网络安全态势的效果有何影响？	• 非常显著的改善	24%
	• 显著改善	31%
	• 几乎没有改善	30%
	• 没有改善	15%
	总计	100%

第 6 部分 其他（请注明）行业实践

Q39a. 贵机构使用怎样的安全测试工具来保证质量？请选择所有的适用项。	• 代码审查 (手工)	30%
	• 静态分析 /SAST(自动)	41%
	• 系统调试	45%
	• 模糊测试	27%
	• 软件组件分析	12%
	• 动态安全测试 /DAST	50%
	• IAST	23%
	• 渗透测试 (跳至 Q39b)	59%
	• 数据脱敏或在测试期间对真实数据进行改动或隐匿	45%
	• 安全补丁管理	61%
	• 运行时应用程序自我保护 (RASP)	31%
	• 威胁建模 (跳至 Q39c)	30%
	• 其他 (请注明)	2%
	总计	456%
Q39b. 如果您选择了渗透测试，渗透测试的目的是什么？	• 确保遵守数据保护条例	26%
	• 通过测试发现安全故障和漏洞	59%
	• 测试应用程序的业务逻辑	15%
	• 其他 (请注明)	0%
	总计	100%
Q39c. 如果您选择了威胁建模，如何实施它？	• 内部安全团队	34%
	• 外部顾问和专家	43%
	• 内外部资源组合	23%
	总计	100%
Q39d. 使用威胁建模的应用程序的百分比是多少？	• 不到 10%	54%
	• 10%-25%	22%
	• 26%-50%	10%
	• 51%-75%	9%
	• 76%-100%	5%
	总计	100%
	推断值	20%

Q40. 贵机构使用哪些工具来评估整个机构安全状况？	• BSIMM	30%
	• OpenSAM	27%
	• 内部评估	64%
	• 其他 (请注明)	7%
	总计	128%

第 7 部分 人口统计信息

D1. 以下哪一项与您目前在贵机构担任的职位最相符？	• 高管	3%
	• 副总裁	5%
	• 总监	13%
	• 经理	20%
	• 主管	12%
	• 工程师	11%
	• 技术员	21%
	• 员工	13%
	• 承包商	2%
	• 其他 (请注明)	0%
	总计	100%
D2. 您或您的直接主管在贵机构中直接受谁领导？	• 首席财务官	5%
	• 首席运营官	4%
	• 总法律顾问	3%
	• DevOps 主管	9%
	• 产品工程主管	7%
	• 质量保证主管	8%
	• 首席信息官	31%
	• 首席技术官	6%
	• 首席信息安全官	16%
	• 首席安全官	3%
	• 合规官	2%
	• 数据中心经理	1%
	• 首席风险官	5%
	• 其他 (请注明)	0%
	总计	100%
D3. 贵机构的总部设在哪里？	• 美国	70%
	• 加拿大	6%
	• 欧洲	13%
	• 中东和非洲	2%
	• 亚太地区	5%
	• 拉丁美洲（包括墨西哥）	4%
	总计	100%

D4. 贵机构的全球员工总数是多少？	• 不到 1,000	21%
	• 1,000-5,000	23%
	• 5,000-10,000	20%
	• 10,001-25,000	21%
	• 25,001-75,000	8%
	• 超过 75,000	7%
	总计	100%

D5. 贵机构今年在网络安全上的花费大约是多少？请选择最接近范围面的技术、人员、管理或外包服务及其他领域 (请注明) 现金支出总投资。	• 无	0%
	• $1-$100,000	0%
	• $100,001- $250,000	2%
	• $250,001 - $500,000	5%
	• $500,001 - $1,000,000	7%
	• $1,000,001 - $2,500,000	9%
	• $2,500,001 - $5,000,000	21%
	• $5,000,001 - $10,000,000	16%
	• $10,000,001 - $25,000,000	21%
	• $25,000,001 - $50,000,000	12%
	• $50,000,001 - $100,000,000	5%
	• 超过 $100,000,000	2%
	总计	100%
	推断值 (US$)	16,544,750

倡导负责任的信息管理

Ponemon Institute 所致力于独立调研和培训，推动企业和政府实施负责任的信息和隐私管理实践。我们的使命是基于实战经验，对影响人员和组织机构之敏感信息管理和安全性的关键问题开展高质量的研究。

我们恪守严格的数据保密、隐私以及符合道德的研究标准。我们不收集任何个人身份信息（或者，在商业调研中，我们不会收集可以确定组织机构身份的信息）。此外，我们还遵循严格的质量标准，以确保不会向受访者询问无关的或不恰当的问题。

如果您有任何疑问，请致函 research@ponemon.org 或致电 800.887.3118 与我们联系。