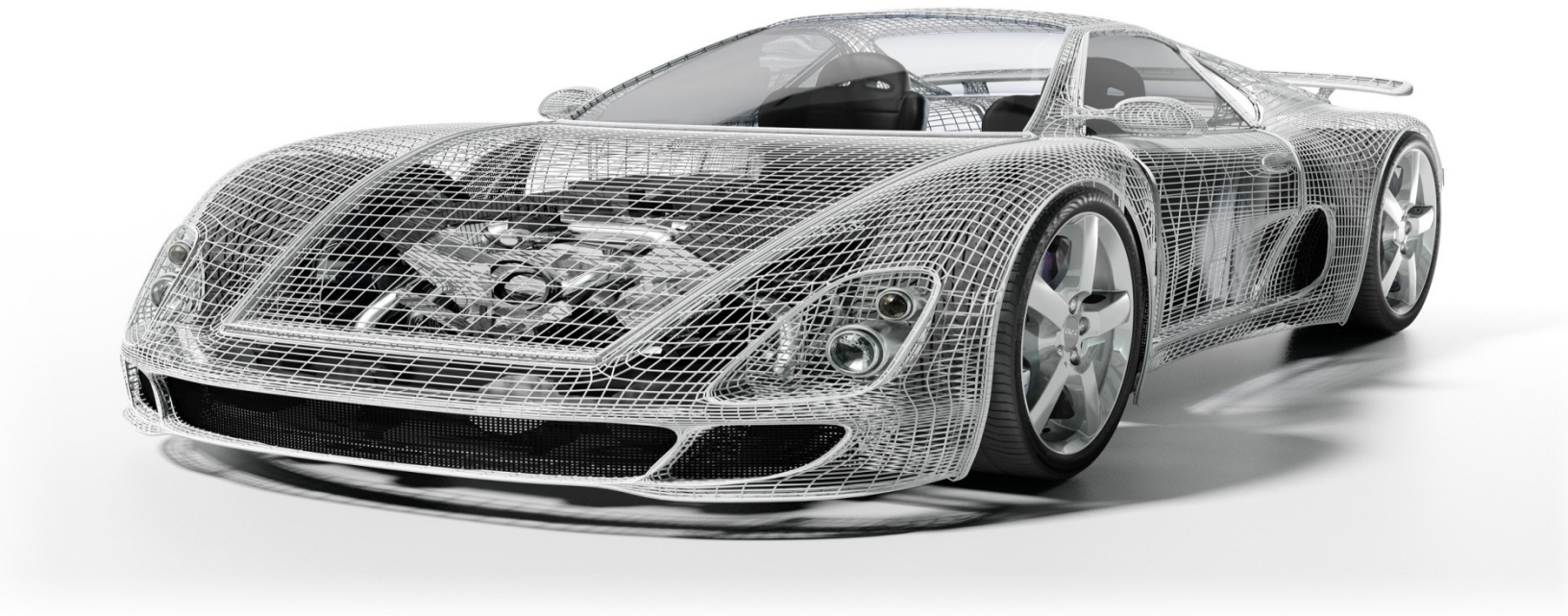
Ponemon INSTITUTE

保护现代车辆的安全：

汽车工业网络安全实践研究



本研究是一项委托进行的独立研究。委托者：

SAE INTERNATIONAL 和 SYNOPSYS®

目录

执行概述

当今的车辆就是一台联网的移动计算机，这带来了一个汽车行业几乎没有什么经验来处理的问题：网络安全风险。汽车制造商面临的软件问题与运输公司没有什么两样，他们都面临着软件安全所固有的各种挑战。

Synopsys 和 SAE International（国际自动机工程师学会）共同委托对汽车行业当前的网络安全实践进行本项独立研究，以填补一项已经存在太长时间的缺口 -- 缺乏相关的数据，无法了解汽车行业的网络安全态势，也无法了解该行业是否具备解决互联的、软件驱动的车辆所固有的软件安全风险。委托 Ponemon 研究所开展了本项研究。研究人员调查了 593 名专业人员，这些人员或者从事汽车零部件的安全性工作，或者评估此类安全性。

软件安全并未与汽车行业的技术发展保持同步

当汽车安全成为软件的一个功能时，软件安全问题就变得至关重要，特别是在涉及联网车辆和自动驾驶汽车等新领域时。然而，正如本报告所示，无论是汽车设备制造商（OEM）或者是他们的供应商，都还在奋力保护在其产品所使用的技术的安全。我们的调查中，有百分之八十四的受访者担心网络安全实践无法匹配不断变化的安全环境。

汽车公司仍然在积累所需要的网络安全技能和资源。在调查中接受访问的安全专业人员表示，通常的汽车企业在其产品网络安全管理项目中只有 9 名全职员工。30％的受访者表示，他们的企业中没有成熟的产品网络安全计划或团队。63％的受访者表示，他们仅仅测试了不到一半的硬件、软件和其他技术来寻找是否存在漏洞。

满足产品截止日期的压力，意外的编码错误，缺乏安全编码实践方面的培训，以及在生产中太晚开展安全漏洞测试，这些都是导致软件漏洞的一些最常见因素。我们的报告表明必须开展以下方面的工作：更加关注网络安全性；开展安全编码培训；获得自动化工具，用于查找源代码中的缺陷和安全漏洞；获得软件组成分析工具，用于发现供应商可能引入的第三方组件。

汽车供应链中的软件存在重大风险

虽然大多数汽车制造商仍然生产某些自研设备，但他们的真正优势在于研发、车辆的设计和营销、零部件供应链的管理以及最终产品的组装。OEM 依靠数百家独立供应商来提供硬件和软件组件，以提供最新的汽车技术和设计。

在我们的报告中，73％的受访者表示，他们非常担心第三方所提供的汽车技术的网络安全状况。但是，只有 44％的受访者表示，他们的企业对上游供应商提供的产品落实了网络安全要求。

联网车辆带来了独特的安全问题

汽车制造商及其供应商还需要考虑联网的汽车对消费者隐私和安全意味着什么。随着越来越多的联网车辆上路，恶意黑客可以利用蜂窝网络、Wi-Fi 和物理连接等途径来访问软件漏洞并加以利用。如果不解决这些风险，将可能酿成代价高昂的错误，包括它们可能对消费者信心、个人隐私和品牌声誉产生不良影响。

在我们调查中的受访者认为，具有最严重风险的技术包括 RF 技术（例如 Wi-Fi 和蓝牙）、车载信息系统（telematics）和自动驾驶（自主）车辆。这表明，非关键性的系统和连接成为攻击者容易得手的目标，它们应该成为网络安全工作的重中之重。

结论

正如下述内容所表明的那样，该行业中无数部门的受访者表现出对网络安全问题的高度认识，并有强烈的改进愿望。值得关注的是，69％的受访者认为他们无力提请他们企业的上级部门关注他们所担忧的问题。但本报告所开展的工作可能有助于让企业高管层和董事会及时看到这些问题。

正如精益制造和 ISO 9000 实践都为汽车行业带来了更高质量一样，要想实现新型汽车技术所具有的全方位优势，同时又要保证质量、安全性和快速上市，严格的网络安全方法至关重要。

组织动态和挑战

尽管受访者看到了明显的危险，但他们并不认为他们有能力把他们对网络安全的担忧提交给更高的管理层。

62%的受访者表示，在未来 12 个月内，很可能或极其有可能出现针对汽车技术的恶意攻击或概念验证攻击；但 69%的受访者表示，他们感到无力把他们担忧的问题提交给上级领导部门。

如图 1 所示，超过一半（52%）的受访者意识到由于不安全的汽车技术而对车辆驾驶员造成的潜在危害，无论这些技术是由第三方开发的还是由其企业自己开发的。但是，只有 31%的受访者表示他们觉得有能力在其组织机构内部提出安全性问题。

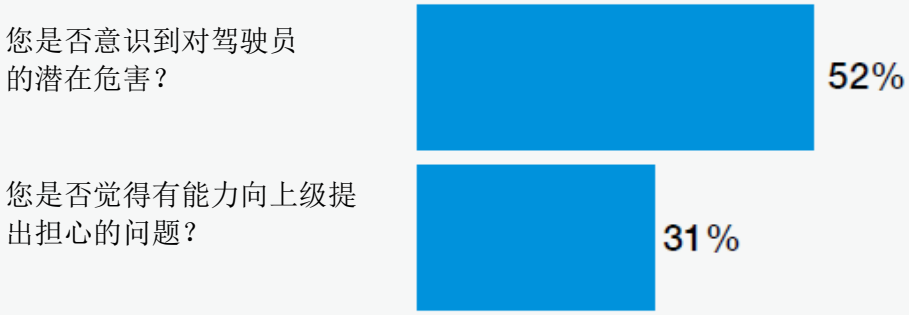


图 1. 人们认识到对驾驶员的潜在危害，但却无法表达出这种担忧。答复“是”的受访者比例

尽管有这些担忧，但缺乏产品网络安全团队和计划。

在您看来，在未来 12 个月内，对于您的企业所开发的或使用的汽车软件/技术/组件而言，发生恶意攻击或概念验证（即安全研究）攻击的可能性有多大？	• ***极其可能***	***27%***
	• ***很可能***	***35%***
	• *某种程度上可能*	23%
	• *不大可能*	15%

您是否觉得有能力在您的组织机构中提出对汽车技术安全性的担忧？	•是	31%
	•***否***	***69%***

30%的受访者表示，他们的企业中没有可靠的产品网络安全计划或团队。只有 10%的受访者表示他们企业拥有一支集中的产品网络安全团队，能够指导和支持多个产品开发团队。

以下哪项最能说明您企业的产品网络安全方法？请仅选择一个选项。	• 产品网络安全是传统 IT 网络安全团队的一部分（通常在全球 CISO[首席信息安全官]的领导之下）	20%
	• 产品网络安全是功能安全团队的一部分	17%
	• 我们有一支集中的产品网络安全团队（即“卓越中心”），其能够指导和支持多个产品开发团队	10%
	• 我们拥有一支分散的产品网络安全团队，网络安全专家隶属于特定的产品开发团队	23%
	• ***我们没有成熟的产品网络安全计划或团队***	***30%***

当依照 OEM 或供应商对这些数据细分时（图 2），可以看出，供应商中 41%的受访者没有任何类型的成熟产品网络安全计划或团队。相比之下，只有 18%的 OEM 没有产品安全计划或团队。

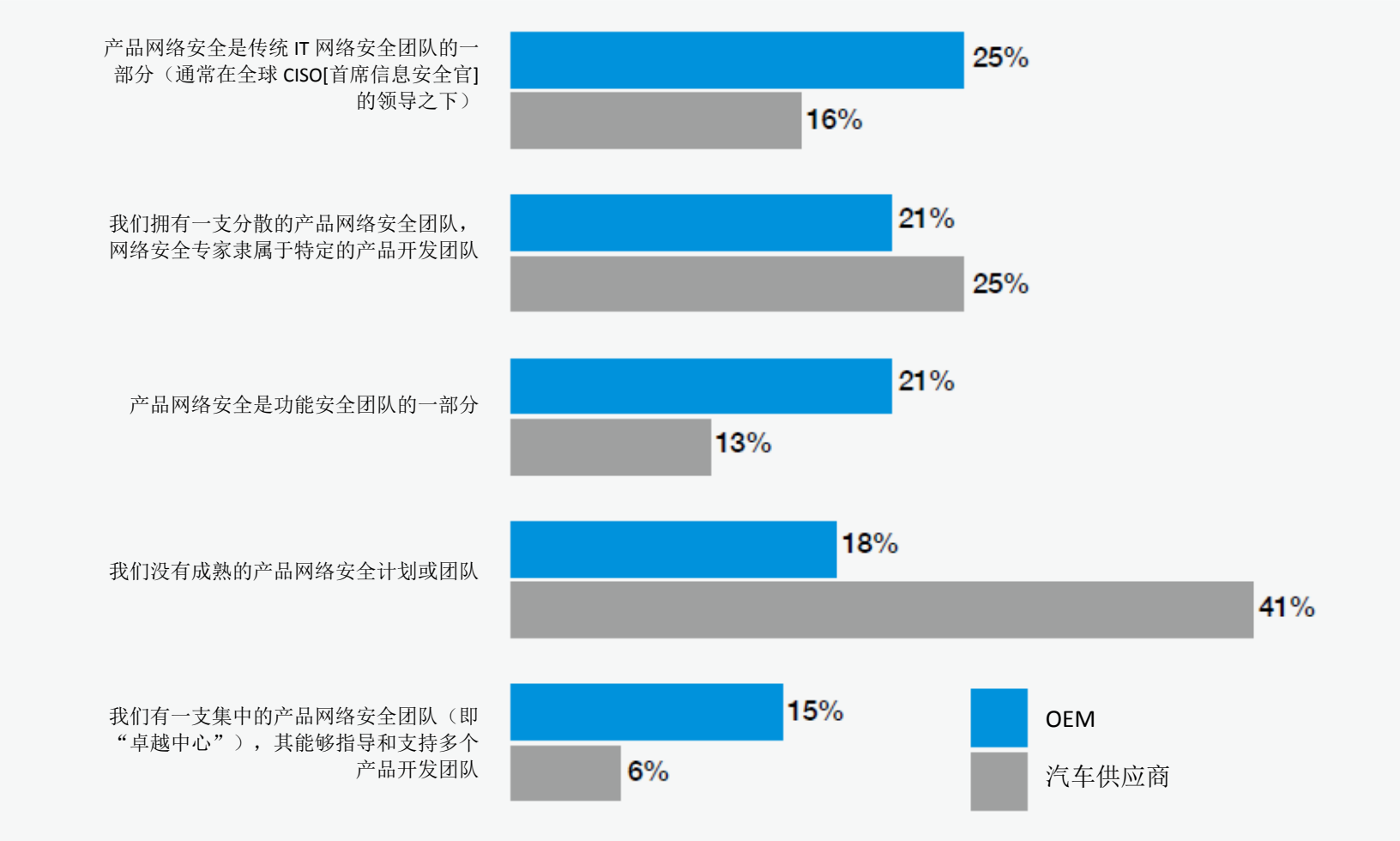


图 2. 以下哪项能够说明您企业的产品网络安全方法？

许许多多的供应商忽略了一项非常成熟的最佳实践：聘请专家团队在从设计阶段到退役的整个产品开发过程中进行安全测试。

汽车公司缺乏必要的网络安全资源和技能。

大多数行业受访者认为，他们不具备足够的资源来应对汽车领域的网络安全威胁。

平均而言，各个企业在其产品网络安全管理项目中只有 9 名全职员工。62%的受访者表示，他们的企业不具备必要的网络安全技能。超过一半（51%）的受访者表示，他们没有足够的预算和人力资本来应对网络安全风险。

您的企业是否为网络安全分配了足够的资源（即预算和人力资源）？	•是	49%
	•否	***51%***
您的企业在产品开发方面是否具备必要的网络安全技能？	•是	38%
	•否	***62%***
有多少 FTE（全职员工）参加您企业的产品网络安全管理项目？	***•少于 5 人***	***30%***
	• 5 至 10 人	***44%***
	• 11 至 20 人	***18%***
	• 超过 20 人	8%

技术动态和挑战

当今的车辆实际上是一个移动的 IT 集合，其包括各种控制系统、丰富的数据、信息娱乐系统以及无线网状通信，它们通过多种协议连接到一起。这种连接可以扩展到驾驶员的个人电子设备中，也可以连接到其他车辆和基础设施中，还可以通过互联网连接到 OEM 和后装市场应用中，从而使其成为网络攻击的目标。未经授权对车辆网络进行远程访问，以及攻击者有可能将目标转向安全关键系统，不仅会使驾驶员的个人信息受到威胁，而且还会危及他们的人身安全。

汽车工程师、产品开发人员以及 IT 专业人员都强调了几个主要的安全问题领域以及他们用于应对风险的安全控制措施。

大多数（84%）的受访者担心，网络安全实践无法跟上技术变化的步伐。

您在多大程度上担忧，您企业的网络安全实践无法跟上不断变化的汽车技术的步伐？ 1=不担心，10=非常担心	• 1 或 2	5%
	• 3 或 4	11%
	• 5 或 6	***25%***
	• 7 或 8	***22%***
	• 9 或 10	***37%***

被认为造成最大风险的技术包括 RF 技术、远程信息处理和自动驾驶车辆。在大踏步进入车辆的各种技术进步中，这三者被认为带来了最大的网络安全风险。企业应该分配更多的资源来降低这些技术中的风险。

受访者表示，导致其技术中出现漏洞的最常见因素包括：满足产品截止日期的压力（71%），缺乏对安全编码实践的理解/培训（60%），以及意外的编码错误（55%）。对关键员工进行安全编码培训将能够应对车辆产生软件漏洞的两个主要因素。

哪些技术构成了最大的网络安全风险？请选择所有符合条件的项目。	•信息娱乐系统	31%
	•动力总成控制单元	46%
	•基于芯片的组件中的 SOC 系统	44%
	•自动驾驶（自主）车辆	***58%***
	•以软件为中心的服务提供商（例如云计算、保险提供商、流媒体服务等）	51%
	•远程信息处理	***60%***
	•转向系统	45%
	•电气化部件	17%
	•摄像头	29%
	•RF 技术（例如 Wi-Fi、蓝牙、热点）	***63%***

导致您的企业开发的或使用的汽车技术中存在漏洞的主要因素是什么？ 请选择最重要的四个因素。	• ***意外的编码错误***	***55%***
	• 使用不安全/过时的开源软件组件	40%
	• 恶意代码注入	23%
	• 缺乏明确规定了安全要求的内部政策或规则	26%
	• ***缺乏对安全编码实践的理解/培训***	***60%***
	• ***满足产品截止日期的压力***	***71%***
	• 缺乏质量保证和测试程序	50%
	• 产品开发工具存在固有缺陷	39%
	• 权限不正确	19%
	• 后端系统	15%

安全补丁和更新是一项挑战。

只有 39％的受访者表示，他们的软件更新交付模式能够及时解决重要的安全漏洞。

您企业的软件更新交付模式是否能够及时解决重要的安全漏洞？	•是	39%
	•*否*	***61%***

如图 3 所示，65％的受访者表示，面向汽车市场的安全补丁和更新是通过所采购的软件、组件和系统来提供的。51％的受访者表示，这项工作是通过连接到个人电子/计算设备的无线通信来完成的。

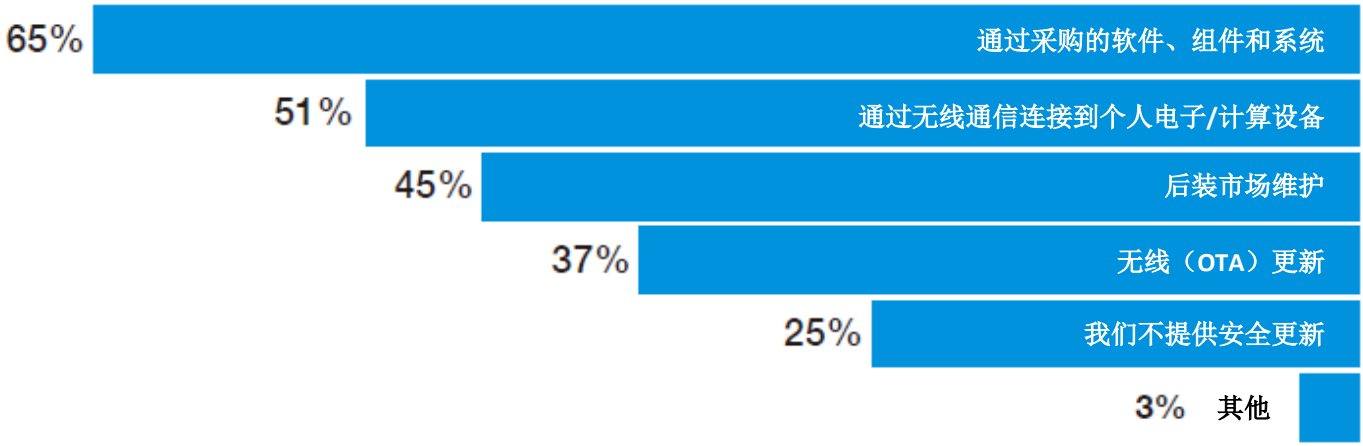


图 3. 您的企业如何完成面向汽车市场的安全补丁和更新？

只有 37%的受访者表示，他们使用无线（OTA）更新方式来提供安全补丁；但超过 50%的受访者表示，他们将在未来 5 年内这样做。这表明需要为安全的 OTA 更新制定一套行业标准。

如果您目前未提供 OTA 更新方式，您是否计划在将来这样做？	*•是的，在 1 至 3 年之内*	*33%*
	•是的，在 3 至 5 年之内	*23%*
	•大于 5 年	*9%*
	• 未计划提供 OTA 更新方式	35%

防火墙和网关是车辆中最常见的安全控制措施。

64%的受访者使用防火墙作为关键安全控制措施，59%的受访者使用网关作为关键安全控制措施。

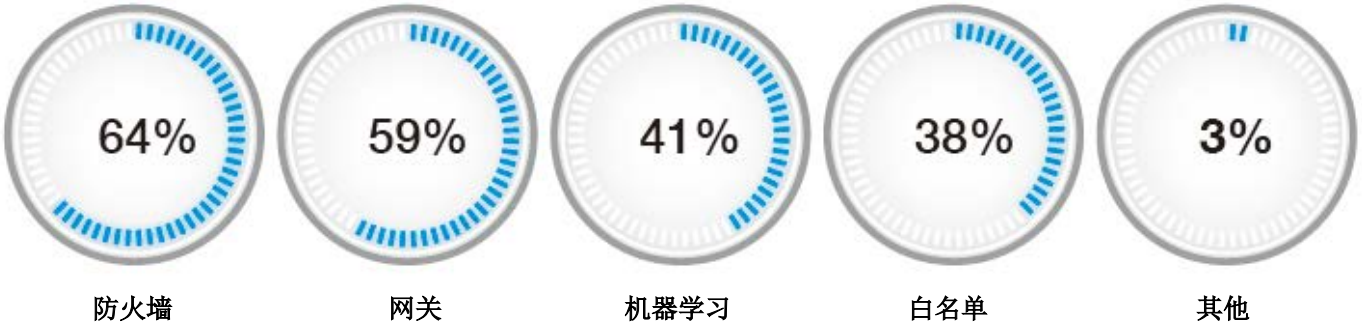


图 4. 您的企业是否在其车辆中采用了安全防范措施？

大多数企业采用了密钥管理系统，但是 43%的企业仍在使用手动流程。

63%的受访者表示，他们的企业采用了密钥管理系统（加密密钥的管理，包括密钥的生成、交换、存储、使用和替换）。如图 5 所示，56%的企业采用了集中的密钥管理系统/服务器，而 45%的企业制定了正式的密钥管理策略。然而，43%的企业使用手动流程进行密钥管理，这限制了其有用性并妨碍了安全性。

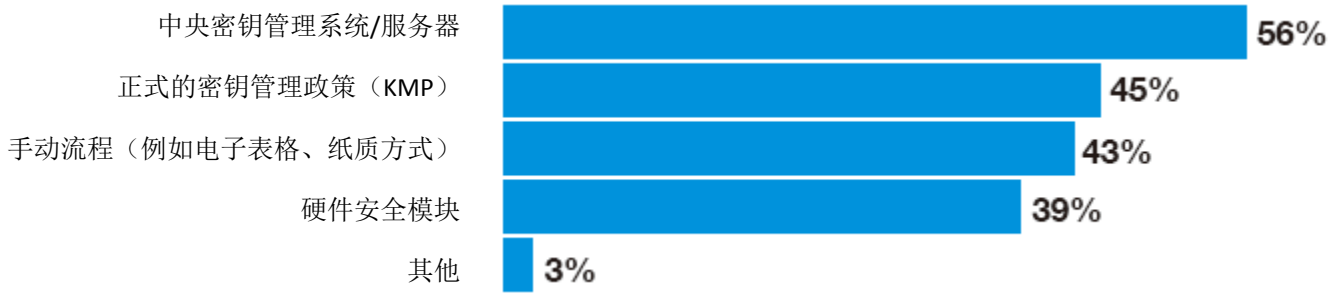


图 5. 您的企业目前在使用什么密钥管理系统？

产品开发和安全测试实践

我们的调查问题针对企业在其产品开发过程中采用的安全实践。成熟的最佳实践采用基于风险的、流程驱动的网络安全方法，并将其整合到整个产品开发生命周期中。

本调查发现，安全漏洞的评估在产品发布过程中进行得太晚了。

只有 47%的企业在“*需求和设计*”阶段或“*开发和测试*”阶段评估漏洞（参见图 6）。

图 6. 在开发生命周期中，您的企业何时评估汽车软件/技术/组件是否存在安全漏洞？

这种流程有悖于 SAE J3061™“*面向网络-物理车辆系统的网络安全指南*”[1]，其要求在整个产品开发生命周期中采用基于风险的、流程驱动的网络安全方法。

将安全性整合到产品开发过程中所带来的优势

1. 将安全概念纳入到产品设计中，能够比在生产之后再采取安全控制措施实现更高的安全性。
2. 能够更早地发现风险和漏洞，并采取适当的安全控制措施。
3. 这是一种更为有效的方式，可以更好地应用有限的网络安全资源，并规范网络安全成本，将其作为产品开发规程中的关键一环。

J3061 是世界上第一部汽车网络安全标准，也是将网络安全流程整合到产品开发过程中的有用工具。

1 *SAE J3061™“面向网络-物理车辆系统的网络安全指南，”*SAE International，2016 年 1 月

未执行足够的安全测试会导致出现漏洞。

百分之六十三的受访者表示，他们仅对不到 50％的硬件、软件和其他技术进行了测试，来确定它们是否存在漏洞。此外，71％的受访者认为，满足产品截止日期的压力是导致出现安全漏洞的主要因素。这些受访答复表明，企业为了满足截止期限的要求，它们仅对极少部分的软件/技术/组件进行了测试。

您的企业所采用的汽车技术中，有多大比例存在漏洞？	***•无***	***25%***
	•低于 25％	***12%***
	• 26％至 50％	***26%***
	• 51％至 76％	***23%***
	• 76％至 100％	14%
	合计	100%
您的企业所使用的不安全的汽车技术会对业务带来哪些负面影响？	•与安全有关的召回	21%
	•供应链合作伙伴关系受到损害	54%
	•延迟或错过发布日期	***67%***
	•在集成测试期间发现组件之间的意外交互	***59%***
	•监管影响、处罚或罚款	5%
	•不知晓任何不良事件	29%
导致您的企业所采用的汽车技术中存在漏洞的主要因素是什么？	•意外编码错误	55%
	•使用不安全的/过时的开源软件组件 40%	40%
	•恶意代码注入	23%
	•缺乏清晰规定安全性要求的内部政策或规则	26%
	•缺乏对安全编码实践的理解/培训	60%
	•满足产品截止日期的压力	***71%***
	•缺乏质量保证及测试程序	50%
	•产品开发工具存在固有缺陷	39%
	•权限不正确	19%
	•后端系统	15%

满足截止期限的压力导致安全测试不足，从而导致出现企业所力图避免的那些漏洞。

漏洞和质量问题是未能始终采用安全的软件开发生命周期（SSDLC）实践所造成的结果之一。

本行业中超过 33%的受访者没有采用公认的 SSDLC 做法，60%的受访者表示他们的企业缺乏对安全编码实践的理解或培训。

您的企业是否遵循了内部或外部发布的关于汽车软件/技术/组件的“安全软件开发生命周期”（SDLC）流程？	•是，内部的	35%
	• 是，外部的	29%
	•否	***36%***

60%的受访者表示，缺乏对安全编码实践的理解/培训导致在汽车软件/技术/组件中出现漏洞。45%的受访者表示，意外编码错误导致在汽车软件/技术/组件中出现漏洞。

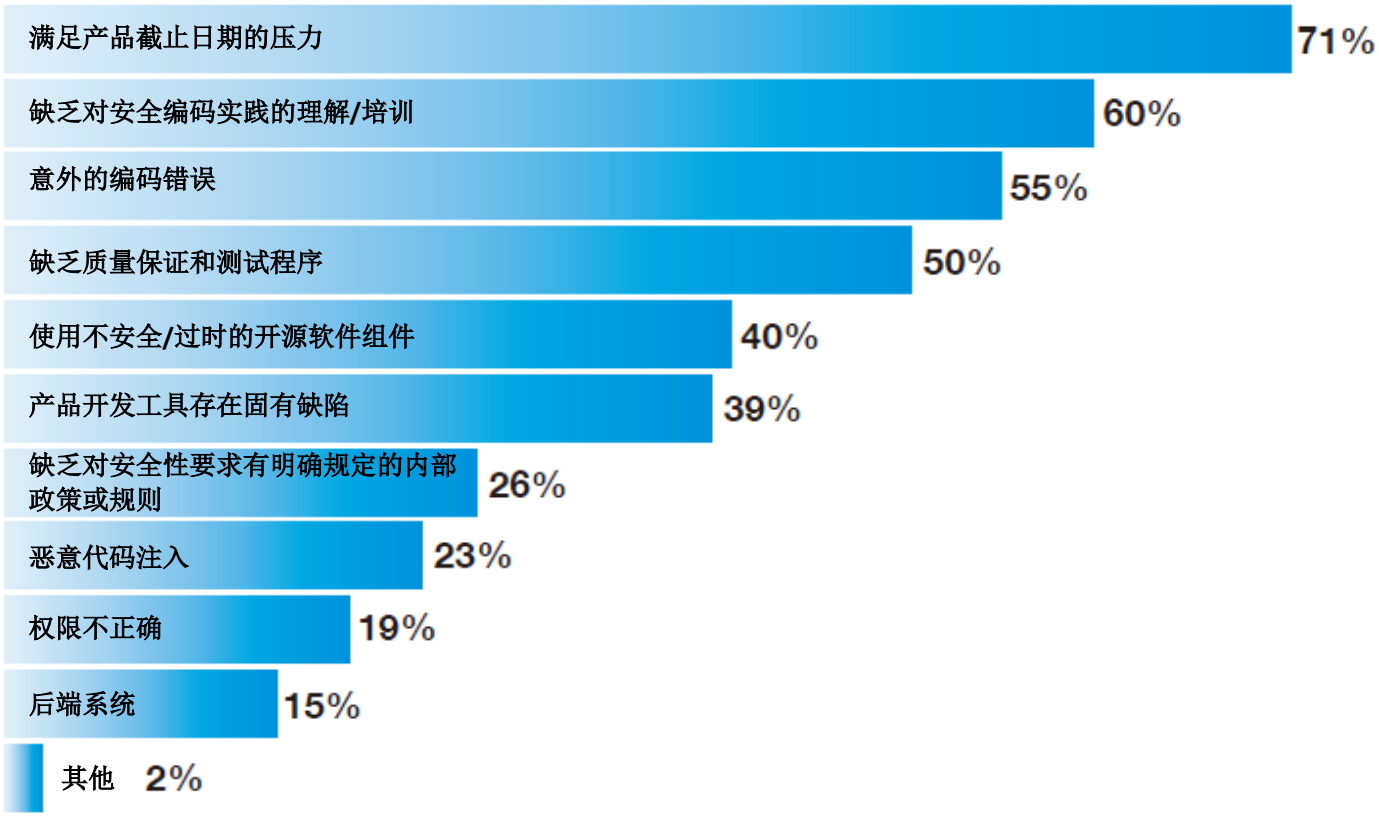


图 7. 导致汽车软件/技术/组件中出现漏洞的主要因素是什么？

业界最常见的安全活动是安全补丁管理、渗透测试以及动态安全测试（DAST）。

受访者表示，保护汽车技术安全最常用的技术手段是安全补丁管理（61％）、渗透测试（56％）和动态安全测试/DAST（49％）。有趣的是，这些都是在生命周期的后期采用的技术。

这再次说明了一个常见问题：网络安全未完全整合到系统开发生命周期中 – 尤其是在早期需求、设计、测试和开发阶段。

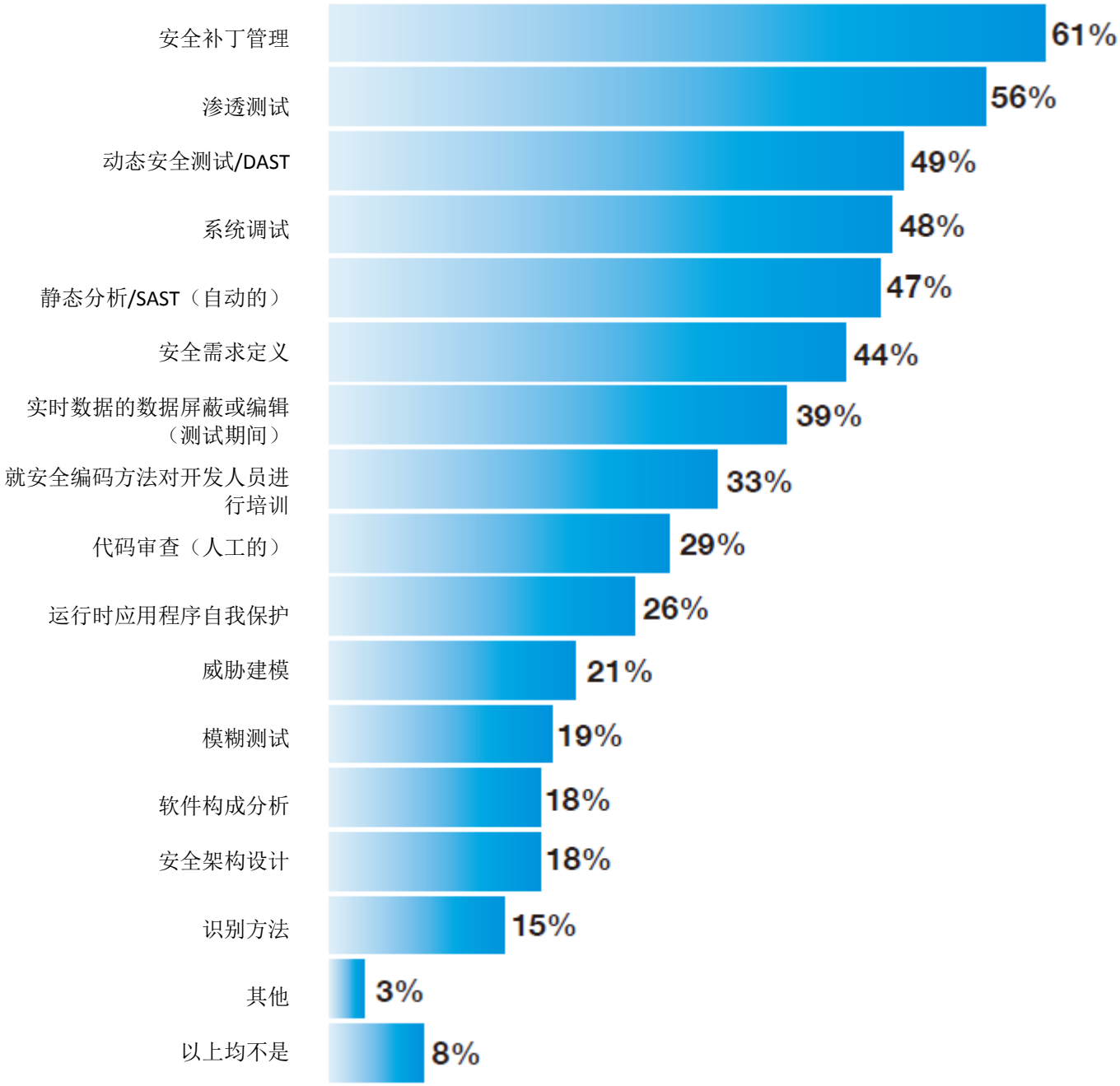


图 8. 您的企业采取了哪些活动来保护汽车软件/技术/组件？

供应链和第三方组件挑战

汽车行业复杂而且迥然不同的供应链是导致质量问题并造成安全漏洞的罪魁祸首。频繁与第三方组件、软件、通信协议和应用程序相集成通常会引入 OEM 必须解决的威胁因素（threat vector）。有几个关键的要点与这些因素有关。

汽车供应链中的漏洞存在重大风险。

73%的受访者非常关注第三方提供的汽车技术的网络安全状况。68%的受访者也非常关注本行业整体上的网络安全状况。

只有 44%的受访者表示，其企业对上游供应商提供的产品提出网络安全方面的要求。制造商应该对其上游供应商的软件、硬件和系统一并提出合适的安全需求以及其他的技术需求。

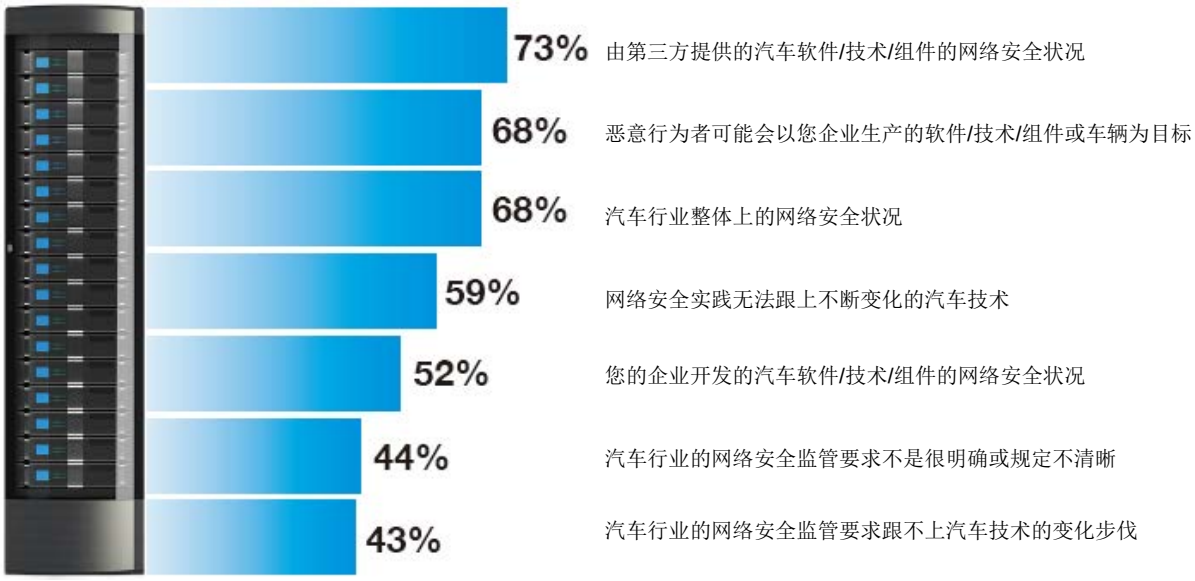


图 9. 对网络安全实践和状况的高度关注
1 =不关注，10 =非常关注，提出 7 个以上的受访答案

安全编码方法方面的培训未被列入优先考虑范围。

只有 33%的受访者表示，他们的企业对开发人员开展安全编码方法方面的培训。60%的受访者表示，缺乏对安全编码实践的理解或培训是导致出现漏洞的主要因素。

您的企业采取哪些活动来保护汽车软件/技术/组件？	***对开发人员进行安全编码方法方面的培训***	***33%***

结论

本次调查的受访者表现出对他们面临的网络安全挑战有显著认识，而且具有改善这一状况的愿望，但他们也同时担心，他们没有能力向高级管理层提出这些问题。受访者对网络安全学科或许最重要的原则有很好的理解：在整个产品开发过程中融入网络安全。

找到人员、流程和技术的恰当组合是取得成功的关键。目前已经有许多解决方案能够加深安全专业人员的能力，无论这些人员目前正在开展安全项目，还是开发高效、有效的安全方法的新手。例如，以下资源可以发挥这些作用：

- SAE J3061™"*面向网络-物理车辆系统的网络安全指南*"描述了一套网络安全流程框架，企业可以以其为基础开发内部网络安全流程，从而设计并把网络安全构筑到车辆系统中。
- 美国国家标准技术研究所（NIST）能够就安全知识和最佳实践提供许多有价值且免费的资源（例如 NIST 特刊 800 系列）。
- 构建安全成熟度模型（BSIMM）和 Synopsys 汽车安全资源页面可以帮助企业制定安全计划，并满足汽车软件的安全性、安保、可靠性和合规性要求。

这些解决方案倡导制定并利用一套基于风险的、流程驱动的方法，把网络安全性与整个产品开发生命周期以及安全软件开发生命周期捆绑到一起。

网络安全培训也是一项重要的投资，不仅能够解决本调查中受访者普遍反映的一个痛点，而且还能够在未来带来红利，并有助于在整个企业中建立安全文化。

汽车行业还拥有许多资源来增强对新出现的安全问题和趋势的理解，并建立专业人员联系网，以及为整个行业的安全做出贡献。

- 汽车信息共享和分析中心（Auto-ISAC）是一个非常有价值的论坛，能够让安全专业人员分享和分析车辆面临的新兴网络安全风险方面的情报，并共同增强汽车行业的网络安全性。
- SAE International 拥有多个制定各种标准、指南和最佳实践的网络安全工作组，提供专业开发培训，并举办各种会议和活动，以便本行业能够及时采用最先进的实践。

通过密切关注开发生命周期的需求阶段，可以应对甚至减轻对本报告中提到的供应链风险的担忧。这可能涉及到与供应商密切合作，以发现组件的设计或架构中的弱点。通过定期审查供应商的网络安全流程，或者在供应商协议中提出网络安全保证要求，可以实现额外的保证。

网络安全不应被视为一个成本中心，也不应当在生产结束时才加以应对，而应当将其纳入系统工程流程的每个步骤中，以指导整个产品开发生命周期 – 尤其是安全软件开发生命周期（SSDLC）。借鉴其他行业已经开发出的指南、最佳实践和标准，汽车公司能够享受到广泛的解决方案。

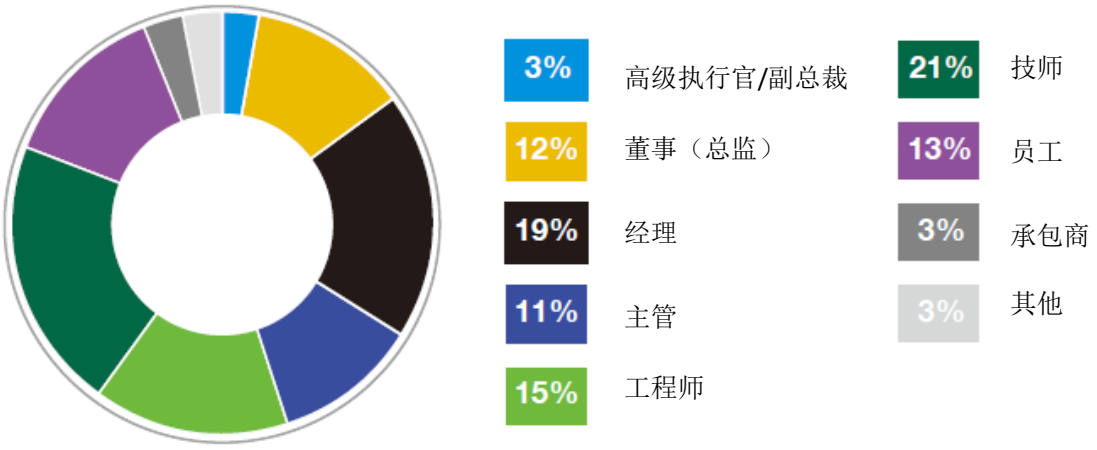
这种实现网络安全的严格方法，对于实现增强的安保能力，同时确保安全性、质量和快速上市，都至关重要。

方法

本次调查的抽样框架由汽车行业的 15,900 名 IT 安全从业人员和工程师组成。为了确保获得有见地的调查应答，所有受访者都参与了为某种汽车零部件的安全性做出贡献或进行评估的工作。表 1 显示了合计 677 个返回的调查答卷（return）。进行筛查和可靠性检查后剔除了 84 份调查表。我们的最终样本包括 593 份调查表，即 3.7%的回复率。

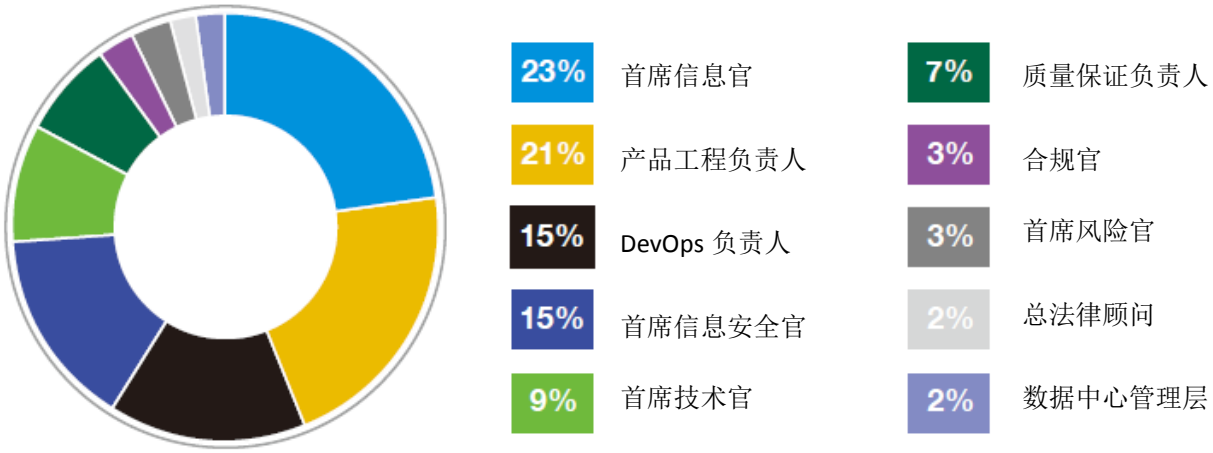
表 1. 样本响应	频度	百分比（%）
• 样本框架合计	15,900	100.0%
• 返回的调查答卷合计	677	4.3%
• 剔除的调查表	84	0.5%
• 最终样本	593	3.7%

饼状图 1 示出了受访者在各自企业中的职位。按设计，超过一半（60%）的受访者担任工程师或更高级别的职位。



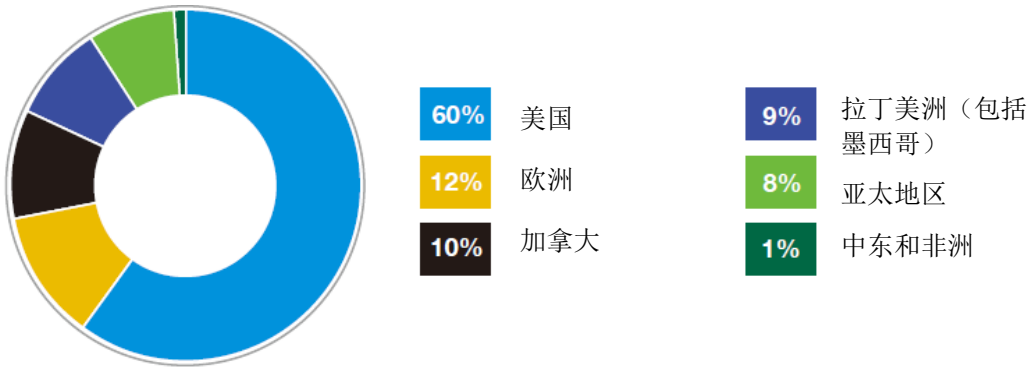
饼状图 1. 目前在企业中担任的职务

如饼状图 2 所示，23%的受访者向首席信息官报告工作，21%向产品工程负责人报告工作，15%向 DevOps 负责人报告工作，15%向首席信息安全官报告工作。



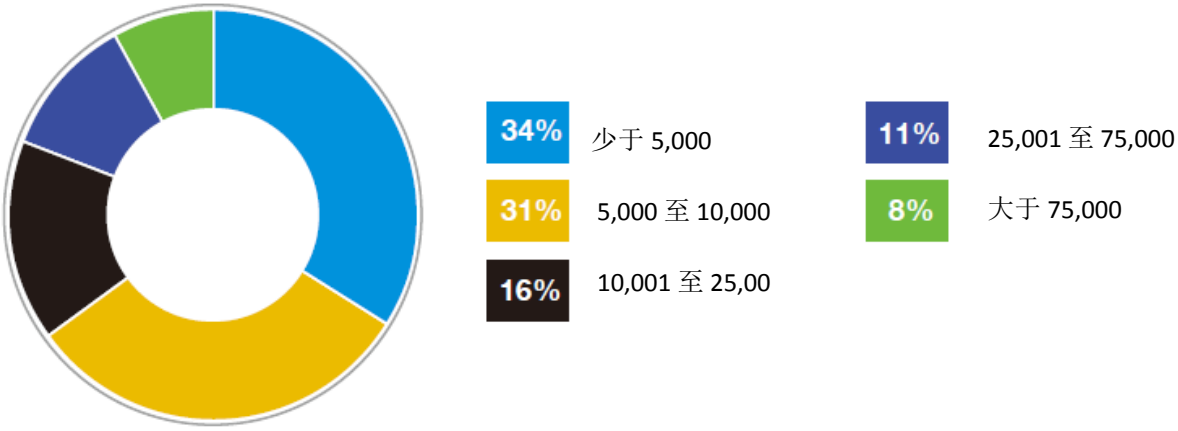
饼状图 2. 您或您的领导报告工作的主要上级

如饼状图 3 所示，大多数受访者的企业（60%）的总部位于美国。另有 12%的企业的总部设在欧洲，还有 10%的总部设在加拿大。



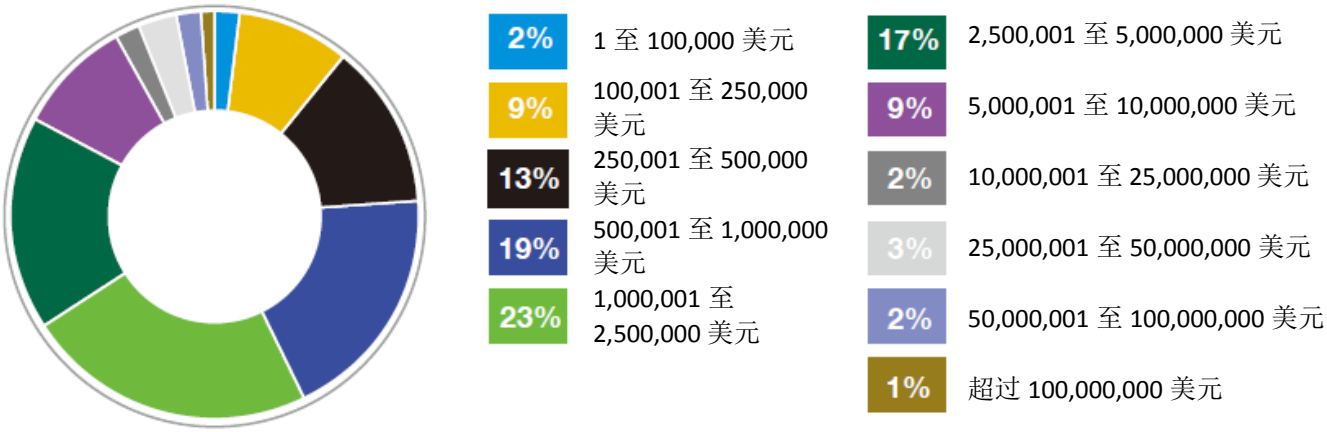
饼状图 3. 企业总部

如饼状图 4 所示，66%的受访者来自全球员工人数超过 5,000 人的企业。



饼状图 4. 企业的全球员工人数

在要求受访者选择最能够描述其企业在技术、人员、管理或外包服务的总投资额以及其他现金支出的大致范围时，57%的受访者表示他们的企业花费超过 100 万美元，如饼状图 5 所示。



饼状图 5. 每年在汽车零部件安全方面的支出。外推值为 6,098,000 美元

关于本项研究的一些注意事项

在从本次调查的结果中得出推论之前，需要仔细考虑本次调查研究的一些固有局限性。以下各项是与大多数基于 Web 的调查密切相关的一些具体限制。

- “无响应”偏差：目前的调查结果以返回的调查问卷样本为基础。我们把调查表发送给有代表性的样本人员，从而产生大量可用的返回的调查表。尽管进行了“无响应”（non- response）测试，但总是存在这样的可能性：未参与调查的人员在基本信念方面与完成了本次调查的人员存在很大差异。

- “抽样框架”偏差：准确性以以下两方面的因素为基础：一是联系人信息是否完善，二是联系人名单对于汽车行业的 IT 安全从业者和工程师在多大程度上具有代表性，即是否能够代表那些为某种汽车组件做出过贡献或参与过相关评估的人员。我们同时也承认，调查结果可能会由于外部事件（例如，媒体报道）的影响而出现偏差。最后，因为我们采用了基于 Web 的收集方法，所以，如果采用邮寄调查问卷或电话呼叫等非 Web 响应方式，可能会导致出现不同的调查结果。

- “自我报告的”结果：调查研究的质量依赖于从受访者那里收到的机密答复信息的完整性。虽然可以在调查过程中采用某些相互制衡的手段，但受访者不提供准确应答信息的可能性总是存在的。

附录：详细的调查结果

下表提供了对本研究中所包含的所有调查问题的回复频度或频度百分比。所有的调查问卷回复均介于 2018 年 7 月 19 日至 2018 年 8 月 3 日之间。

样本响应	频度	百分比（%）
• 样本框架合计	15,900	100.0%
• 返回的调查答卷合计	677	4.3%
• 剔除的调查表	84	0.5%
• 最终样本	593	3.7%

第 1 部分. 筛选

S1a. 在为汽车组件的安全性做出贡献或开展评估方面，您是否担任任何角色或参与了相关工作？	• 是的，广泛参与	32%
	• 是的，有些参与	50%
	• 是的，少量参与	18%
	• 没有参与（停止）	0%
	合计	100%

如果您参与了相关工作的话，您为汽车设备的安全性做出贡献或进行评估有多少年的时间？	• 不到 1 年	8%
	• 2 至 4 年	25%
	• 5 至 7 年	33%
	• 8 至 10 年	19%
	• 超过 10 年	15%
	• 无法确定（停止）	0%
	合计	100%
	外推值	6.31

S2. 以下哪项最能够说明您的企业在汽车技术和/或组件开发中发挥的作用？	• 供应商	21%
	• 制造商	50%
	• 服务提供商	29%
	• 以上都不是（停止）	0%
	合计	100%

第 2 部分. 背景和组织动态

Q1. 以下哪项最能够说明您的企业在汽车行业中的地位？	• 原始设备制造商(OEM)	47%
	• 第 1 层	36%
	• 第 2 层	12%
	• 第 3 层或更高	3%
	• 其他	2%
	合计	100%

Q2. 您的企业目前大约制造多少种不同类型的汽车零部件或产品？	• 低于 5 种	19%
	• 6 至 25 种	34%
	• 26 至 50 种	30%
	• 超过 50 种	17%
	合计	100%
	外推值	27.63
Q3. 您的企业设计和开发什么类型的汽车软件/技术/组件？请选择所有适用的选项。	• 信息娱乐系统	31%
	• 动力总成控制单元	37%
	• 基于芯片的组件上的 SOC 系统	17%
	• 自动驾驶（自主）车辆	40%
	• 以软件为中心的服务提供商（例如云计算、保险提供商、流媒体服务等）	30%
	• 远程信息处理	49%
	• 转向系统	21%
	• 电气化部件	36%
	• 摄像头	28%
	• RF 技术（例如 Wi-Fi、蓝牙、热点）	46%
	• 其他（请注明）	2%
Q4. 以下哪项最能够说明您企业的产品网络安全方法？请仅选择一个选项。	产品网络安全是传统 IT 网络安全团队的一部分（通常在一位全球 CISO 的领导下）	20%
	产品网络安全是功能安全团队的一部分	17%
	我们拥有一支集中的产品网络安全团队（即卓越中心），其负责指导和支持多个产品开发团队	10%
	我们拥有一支分散的产品网络安全团队，网络安全专家隶属于特定的产品开发团队	23%
	我们没有成熟的产品网络安全计划或团队	30%
	合计	100%
Q5. 您企业中有多少全职员工（FTE）参与产品网络安全管理计划？	• 5 少于 5 人	30%
	• 5 至 10 人	44%
	• 11 至 20 人	18%
	• 超过 20 人	8%
	合计	100%
	外推值	9.21
Q6. 您的企业是否为网络安全分配了足够的资源（即预算和人力资源）？	• 是	49%
	• 否	51%
	合计	100%

Q7. 您的企业在产品开发方面是否具备必要的网络安全技能？	• 是	38%
	• 否	62%
	合计	100%

Q8. 您是否觉得有能力在您的企业中提出对汽车技术安全性的担忧？	• 是	31%
	• 否	69%
	合计	100%

第 3 部分. 对汽车行业中软件安全风险的看法

Q9. 哪些技术构成了最大的网络安全风险？请选择所有适用的选项。	• 信息娱乐系统	31%
	• 动力总成控制单元	46%
	• 基于芯片的组件中的 SOC 系统	44%
	• 自动驾驶（自主）车辆	58%
	• 以软件为中心的服务提供商（例如云计算、保险提供商、流媒体服务等）	51%
	• 远程信息处理	60%
	• 转向系统	45%
	• 电气化组件	17%
	• 摄像头	29%
	• RF 技术（例如 Wi-Fi、蓝牙、热点）	63%
	• 其他（请注明）	2%

Q10. 您是否了解由于您的企业所开发的或使用的不安全的汽车软件/技术/组件而造成的以下任何负面业务影响？请选择所有适用的选项。	• 与安全有关的召回	21%
	• 供应链合作伙伴关系受损	54%
	• 延迟或错过发布日期	67%
	• 在集成测试期间出现组件之间的意外交互	59%
	• 监管影响、处罚或罚款	5%
	• 不知悉任何不良事件	29%

Q11. 您是否了解由于您的企业开发的或使用的不安全的汽车软件/技术/组件对车辆驾驶员造成的任何潜在危害？	• 是	52%
	• 否	48%
	合计	100%

Q12. 在您看来，在未来 12 个月内，您的企业开发的或使用的汽车软件/技术/组件遭受恶意攻击或概念验证（即安全研究）攻击的可能性有多大？	• 极其可能	27%
	• 很可能	35%
	• 某种程度上可能	23%
	• 不大可能	15%
	合计	100%

请以 10 分为标准对以下陈述打分。1=不担忧，10=非常担忧。

Q13. 您对您企业开发的汽车软件/技术/组件的网络安全状况担忧程度如何？	• 1 或 2 分	13%
	• 3 或 4 分	12%
	• 5 或 6 分	23%
	• 7 或 8 分	26%
	• 9 或 10 分	26%
	合计	100%
	外推值	6.30
Q14. 您对第三方开发的汽车软件/技术/组件的网络安全状况担忧程度如何？	• 1 或 2 分	8%
	• 3 或 4 分	4%
	• 5 或 6 分	15%
	• 7 或 8 分	30%
	• 9 或 10 分	43%
	合计	100%
	外推值	7.42
Q15. 您对汽车行业整体上的网络安全状况担忧程度如何？	• 1 或 2 分	9%
	• 3 或 4 分	6%
	• 5 或 6 分	17%
	• 7 或 8 分	28%
	• 9 或 10 分	40%
	合计	100%
	外推值	7.18
Q16. 您对您企业的网络安全实践无法跟上不断变化的汽车技术的担忧程度如何？	• 1 或 2 分	5%
	• 3 或 4 分	11%
	• 5 或 6 分	25%
	• 7 或 8 分	22%
	• 9 或 10 分	37%
	合计	100%
	外推值	7.00

Q17. 您对汽车行业的网络安全监管要求无法跟上不断变化的汽车技术的担忧程度如何？	• 1 或 2 分	12%
	• 3 或 4 分	16%
	• 5 或 6 分	29%
	• 7 或 8 分	23%
	• 9 或 10 分	20%
	合计	100%
	外推值	5.96
Q18. 您对汽车行业的网络安全监管要求不是很明晰或规定不明确的担忧程度如何？	• 1 或 2 分	10%
	• 3 或 4 分	19%
	• 5 或 6 分	27%
	• 7 或 8 分	25%
	• 9 或 10 分	19%
	合计	100%
	外推值	5.98
Q19. 您对恶意行为者可能以您企业生产的软件/技术/组件或车辆为目标的担忧程度如何？	• 1 或 2 分	15%
	• 3 或 4 分	7%
	• 5 或 6 分	10%
	• 7 或 8 分	33%
	• 9 或 10 分	35%
	合计	100%
	外推值	6.82
Q20. 对于您的企业在把汽车软件/技术/组件推向市场之前能够检测到其中的安全漏洞，您有多大信心？	• 1 或 2 分	44%
	• 3 或 4 分	25%
	• 5 或 6 分	12%
	• 7 或 8 分	4%
	• 9 或 10 分	15%
	合计	100%
	外推值	3.92
Q21. 在把汽车软件/技术/组件推向市场之前检测其中的安全漏洞，您的企业面临多大困难？	• 1 或 2 分	7%
	• 3 或 4 分	5%
	• 5 或 6 分	23%
	• 7 或 8 分	25%
	• 9 或 10 分	40%
	合计	100%
	外推值	7.22

Q22. 您的企业有多迫切的需要在汽车软件/技术/组件中应用与网络安全相关的控制措施？	• 1 或 2 分	10%
	• 3 或 4 分	10%
	• 5 或 6 分	13%
	• 7 或 8 分	41%
	• 9 或 10 分	26%
	合计	100%
	外推值	6.76

Q23. 以下任何因素会影响您的企业增加预算吗？请选择最重要的两项因素。	• 新法律法规	35%
	• 漏洞研究人员披露的信息	49%
	• 您企业的某个汽车组件发生严重的黑客入侵事故	54%
	• 强制召回	60%
	• 其他（请注明）	2%
	• 以上均不是	0%

第 4 部分. SDLC 方面的安全实践

Q24a. 您的企业是否为其软件开发人员提供安全开发培训？	• 是的，它是可选的	21%
	• 是的，它是强制性的	25%
	• 是的，仅限某些团队	24%
	• 没有，我们不提供安全开发培训	30%
	合计	100%

Q24b. 如果提供的话，您企业的安全开发培训效果如何？	• 极其有效	15%
	• 很有效	21%
	• 某种程度上有效	24%
	• 没有效果	40%
	合计	100%

Q25. 您的企业是否遵循内部或外部发布的关于汽车软件/技术/组件的“安全软件开发生命周期（SSDLC）”流程？	• 是的，内部发布的	35%
	• 是的，外部发布的	29%
	• 否	36%
	合计	100%

Q26. 平均而言，您企业开发的或使用的汽车软件/技术/组件中有多大比例针对网络安全漏洞进行了测试？	没有	25%
	低于 25%	12%
	26%至 50%	26%
	51% 至 75%	23%
	76% 至 100%	14%
	合计	100%
	外推值	39%

Q27. 在开发生命周期中，您的企业什么时候评估汽车软件/技术/组件的安全漏洞？请选择所有适用的选项。	• 需求和设计阶段	19%
	• 开发和测试阶段	28%
	• 发布后阶段	43%
	• 集成到车辆网络之后	37%
	• 生产发布之后	18%
Q28. 您的企业开展哪些活动来保护汽车软件/技术/组件的安全？请选择所有适用的选项。	• 就安全编码方法对开发人员进行培训	33%
	• 安全架构设计	18%
	• 威胁建模	21%
	• 识别方法	15%
	• 安全需求定义	44%
	• 代码审查	29%
	• 静态分析/SAST（自动的）	47%
	• 系统调试	48%
	• 模糊测试	19%
	• 软件构成分析	18%
	• 动态安全测试/DAST	49%
	• 渗透测试	56%
	• 实时数据的数据屏蔽或编辑（测试期间）	39%
	• 安全补丁管理	61%
	• 运行时应用程序自我保护	26%
	• 其他（请注明）	3%
	• 以上均不是	8%
Q29. 您企业在其开发的汽车软件/技术/组件中是否使用开源代码？	• 是的，我们有一套既定流程来存储和管理所使用的开源代码	26%
	• 是的，我们使用开源代码，但没有一套既定的流程来存储和管理对开源代码的使用	32%
	• 否，我们不使用开源代码	42%
	合计	100%
要因素是什么？请选择最重要的四项因素。	• 意外编码错误	55%
	• 使用不安全的/过时的开源软件组件	40%
	• 恶意代码注入	23%
	• 缺乏对安全性要求有明确规定的内部政策或规则	26%
	• 缺乏对安全编码实践的理解/培训	60%
	• 满足产品截止日期的压力	71%
	• 缺乏质量保证和测试程序	50%
	• 产品开发工具存在固有错误	39%
	• 权限不正确	19%
	• 后端系统	15%
	• 其他（请注明）	2%

Q31. 在发生严重漏洞披露时，您公司是否制定了事件响应计划？	• 是	43%
	• 否	57%
	合计	100%
Q32. 您公司是否在其车辆中整合了任何安全措施？请选择所有适用的项目。	• 网关	59%
	• 防火墙	64%
	• 机器学习	41%
	• 白名单	38%
	• 其他（请注明）	3%
Q33a. 您公司是否针对开发或制造过程中使用的软件/技术/组件采用了密钥管理系统？	• 是	63%
	• 否	37%
	合计	100%
Q33b. 如果是的话，您的企业目前在使用哪些密钥管理系统？请选择所有适用的项目。	• 正式的密钥管理政策（KMP）	45%
	• 手动流程（例如电子表格、纸质方式）	43%
	• 中央密钥管理系统/服务器	56%
	• 硬件安全模块	39%
	• 其他	2%
Q34. 您的企业如何为市场上的车辆提供安全补丁和更新？	• 无线（OTA）更新	37%
	• 后装市场维护	45%
	• 通过无线通信连接到个人电子/计算设备	51%
	• 通过采购的软件、组件和系统	65%
	• 我们不提供安全更新	25%
	• 其他	3%
Q35. 如果您公司现在未提供 OTA 更新，未来打算这样做吗？	• 是，1 至 3 年内	33%
	• 是，3 至 5 年内	23%
	• 5 年以后	9%
	• 没有计划提供 OTA 更新	35%
	合计	100%
Q36. 您公司的软件更新交付模型是否能够及时解决重大安全漏洞？	• 是	39%
	• 否	61%
	合计	100%

第 5 部分. 网络安全供应链实践

Q37a. 您公司是否对上游供应商提供的汽车软件/技术/组件提出了网络安全要求？	• 是	44%
	• 否（跳至 Q38）	56%
	合计	100%
Q37b. 如果是的话，您的企业如何确保这些供应商遵守相关安全性要求？请选择所有适用的项目。	• 要求供应商进行自我评估并提供验证和确认书	51%
	• 要求第三方进行评估并提供独立的验证和确认书	25%
	• 我们直接进行供应商安全评估	38%
	• 在供应商协议中明确规定安全要求	49%
	• 我们没有正式的流程来确保供应商遵守安全要求（跳至 Q38）	40%
Q37c. 如果是的话，您的企业以多大频度要求供应商提供安全保证？	• 每年一次	33%
	• 每季度一次	9%
	• 每次有重大版本发布时	26%
	• 每次发生代码变更时	29%
	• 其他	3%
	合计	100%

第 6 部分. 未来的汽车行业实践

Q38. 什么样的未来网络架构能够增强车辆安全性？	• 汽车以太网	44%
	• 标准	50%
	• 5G 网络	54%
	• 其他（请注明）	8%
	• 以上都不是	26%
哪些有针对性的标准/指南/技术将创建出更安全/更具弹性的车辆网络？	• 安全模块	29%
	• 网关	50%
	• IDS 入侵检测系统（IDS）	54%
	• 安全的 OTA 更新	63%
	• 白名单	47%
	• 其他（请注明）	5%

Q40. 什么是最有效的、最易于实现的安全保证测试/认证/鉴定方法？	• 自我认证	20%
	• 符合某种流程标准的自我认证	40%
	• 自我认证，并进行定期评估	32%
	• 型式认证	8%
	• 其他（请注明）	0%
	合计	100%

第 7 部分. 人口统计和组织特征

D1. 哪种组织级别最能够描述您当前的职位？	• 高级执行官/副总裁	3%
	• 董事（总监）	12%
	• 经理	19%
	• 主管	11%
	• 工程师	15%
	• 技师	21%
	•员工	13%
	• 承包商	3%
	• 其他	3%
	合计	100%

D2. 请选择您或您的领导者在企业内向上级报告工作的主要人员。	• 首席财务官	0%
	• 首席运营官	0%
	• 总法律顾问	2%
	• DevOps 负责人	15%
	• 产品工程负责人	21%
	• 质量保证负责人	7%
	• 首席信息官	23%
	• 首席技术官	9%
	• 首席信息安全官	15%
	• 首席安全官	0%
	• 合规官	3%
	• 数据中心管理层	2%
	• 首席风险官	3%
	• 其他	0%
	合计	100%

D3. 您公司总部在哪里？	• 美国	60%
	• 加拿大	10%
	•欧洲	12%
	•中东和非洲	1%
	• 亚太地区	8%
	• 拉丁美洲（包括墨西哥）	9%
	合计	100%

D4. 您公司的全球员工人数有多少？	• 少于 5,000	34%
	• 5,000 至 10,000	31%
	• 10,001 至 25,000	16%
	• 25,001 至 75,000	11%
	• 大于 75,000	8%
	合计	100%

D5. 您的企业每年在汽车组件安全方面的支出大约是多少？请选择在技术、人员、托管或外包服务以及其他现金支出方面最接近的总投资额。	• 无	0%
	• 1 至 100,000 美元	2%
	• 100,001 至 250,000 美元	9%
	• 250,001 至 500,000 美元	13%
	• 500,001 至 1,000,000 美元	19%
	• 1,000,001 至 2,500,000 美元	23%
	• 2,500,001 至 5,000,000 美元	17%
	• 5,000,001 至 10,000,000 美元	9%
	• 10,000,001 至 25,000,000 美元	2%
	• 25,000,001 至 50,000,000 美元	3%
	• 50,000,001 至 100,000,000 美元	2%
	• 超过 100,000,000 美元	1%
	合计	100%
	外推值（美元）	$6,098,000

推进负责任的信息管理

Ponemon Institute（Ponemon 研究所）致力于开展独立的研究和教育，以期在企业和政府部门中推进负责任的信息和隐私管理实践。我们的使命是：在关于人员和组织机构的敏感信息方面，就影响其管理和安全性的关键问题进行高质量的实证研究。

我们坚持严格的数据保密、隐私和道德研究标准。我们不会从个人那里收集任何可识别个人的信息（在我们的商业业务研究中，也不会收集任何可识别企业的信息）。此外，我们制定了严格的质量标准，以确保不会向受访者提出外在的、无关的或不恰当的问题。

如果有任何疑问，请联系 research@ponemon.org 或致电 800.887.3118。