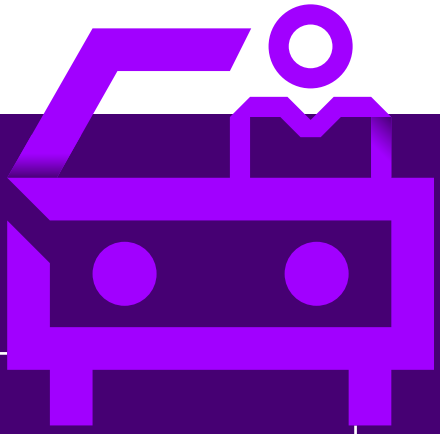
accenture consulting
埃森哲咨询

掌控网络安全的方向盘

构建汽车行业的网络弹性

加强网络安全

任何行业都无法躲开网络攻击的威胁，概莫能外。汽车企业去年遭受将近160次有针对性的攻击，雪上加霜的是还要应对复杂的商业模式，包括处理遗留系统，庞大的供应商交付网络和新数据的需求。如今全球互联日益紧密，汽车业首席信息安全官面临的挑战是保护企业关键IT和生产系统免受网络攻击，同时还要应对一些未来威胁，比如来自更广阔的生态系统关系和不断增长的海量数据而导致的隐患。这些举措改变了首席信息安全官的职责范围，由原先以技术见长的专家转型为专注于业务成果的顾问。为了实现这一转变，首席信息安全官不仅需要加强与首席数字官和数字营销团队的合作，还应具备抵御网络威胁和加速企业竞争优势所需的洞察力和远见。



81% 汽车业高管相信，在发生网络攻击时，他们能够迅速恢复生产运营；其中有关网络安全能力的调查显示，汽车行业在所有33项中有18项表现出色。

2/3 汽车业高管在受访中表示经历过安全事故，其中64%涉及客户个人身份信息安全，63%涉及制造商工业控制系统的安全事故。

业务优先的安全策略

首席信息安全官需要成为业务推动者和网络安全战略的守护者，来保护关键资产和运营，即使在企业转型期间，依然加强竞争力并推动增长。互联的环境、更广泛的生态系统以及业务各方面不断扩展的数据应用必然会导致安全隐患，企业应当对这些即将来临的威胁未雨绸缪。简而言之，安全团队必须处于任何战略计划的前沿和中心。

网络安全预算的授权由企业最高层决定；相比全球所有行业受访者，更多汽车行业的受访者认为与董事会成员决策有关。

30%
汽车行业受访者

27%
全球所有行业受访者

汽车制造商可以采取下列行动，重塑传统运营以应对下一波网络威胁，包括：

- **确保运营技术环境安全**
- **保障供应链安全**
- **业务从以产品为导向转向以客户为中心**

确保运营技术环境安全

数字化时代，生产环境将面临很多新的威胁。因此首席信息安全官必须将职责范围扩展到信息技术（IT）环境之外。随着运营技术环境日益互联，企业也就更加容易受到攻击。例如，当NotPetya病毒袭击网络时，恶意软件从乌克兰软件公司的服务器蔓延到全球一些最大的企业，使其运营陷入瘫痪，并造成约100亿美元的损失。[1] 类似事件，恶意软件WannaCry迫使多家汽车制造商的一些欧洲工厂停产，甚至还关闭了其中一间。因此安全性必须无缝衔接，并且可以普遍适用于整个企业，如果决策制定没有基于可持续的安全规划和实践，这将对车企的业务、声誉和市场份额产生重大影响。随着汽车行业广泛采用产业物联网（IIoT），一旦运营环境受到攻击，流程控制设备或采用机器人控制单元的生产线也会立即受到影响。从企业和技术角度来看，这些威胁足以对整个行业构成挑战。

保护知识产权和避免停产是所有汽车制造商的首要任务。安全目标需要着重关注三个方面：

可用性：生产环境中发生业务中断，对企业而言是灾难性的。如果无法正确管理可用性，即时生产系统可能会立即造成重大财务损失。

完整性：针对工厂数据完整性的网络攻击，可能会造成整车厂采取影响深远的回调举措。

机密性：日益增长的数字化和规范化需求更需要有效的数据保护。汽车制造商如果没有将数据保护放在首位，可能会失去客户信任，甚至面临巨额罚款。汽车制造商应当在产品生命周期的早期就将数据保护纳入考虑范畴，并且平衡运营环境中可访问数据的需求和限制。

71%

汽车业高管还未认识到新业务模式带来的风险和增加的攻击面，这个比例低于全球受访者（82%）。

信息技术（IT）和运营技术（OT）需求的融合凸显了两者之间巨大的差异。安全团队尚不熟悉运营技术，而运营团队的成员在处理网络安全问题时，也没有相关的问责制和流程化专业知识。运营技术系统的平均使用寿命通常为15至20年，而信息技术系统的平均寿命则为3至5年。且运营技术系统的更新和补丁并不频繁，需要与为数不多的维护窗口保持一致性，并仔细管理避免运营中断。最后，与信息技术环境不同，运营技术环境的网络通常没有得到适当的分区和保护，使攻击者能够在整个环境中进行横向移动攻击。随着汽车行业的参与者准备像其他行业的企业一样打造未来生产方式，如通用电气就构建了一支使用人工智能技术的数字孪生“军队”，以期大幅节省运营成本，[2] 就更需要确保自己在安全的环境中开展运营。

保障供应链安全

除了内部的安全控制，汽车制造商有责任将安全性延展到合作伙伴和供应商的生态系统中，这也是其业务运营不可或缺的一部分，特别是对于那些需要访问关键系统和数据的合作伙伴。在高度分散的生产环境中，一些汽车制造商依赖第三方生产的产品比例已高达70%，这种情形下的合作关系更需要透明度和信任度。一辆汽车由5,000多个可更换零部件构成，涉及逾千家外部供应商来制造这些不同种类的零部件。为了配合提供这些产品，供应商需要访问一些制造商的知识产权（IP）以及支持定制的客户数据。但是37%的汽车企业表示，他们并未将相同的安全标准应用于他们的合作伙伴。[3] 较小的制造商和供应商平时采取的安全措施远低于产品供应所需的安全措施。与其他行业不同，除了供应商之外，车企还有一个包含成千上万经销商和销售代表的分销网络。因此确保网络完全，避免黑客针对最薄弱环节的攻击是一项巨大的挑战。过去五年中，越来越多的证据表明存在这一弱点攻击现象。举例来说，有人利用网络浏览器中的弱点，对特定车型的驾驶和停车模式的一些系统进行远程控制，甚至损害整个汽车系统，便于其解锁车辆甚至启动发动机。2018年7月，一名安全研究人员通过一家小型加拿大公司获取了几乎所有主要车企的公司敏感文件，这些车企均与该加拿大公司有过合作。这次入侵并非网络攻击导致，而是由于内部服务器上的密码缺失保护，属于企业内部在安全基础上的缺陷。

50% 汽车业高管认为其第三方合作伙伴的网络安全表现优异，这一比例比全球受访者总体低9%。

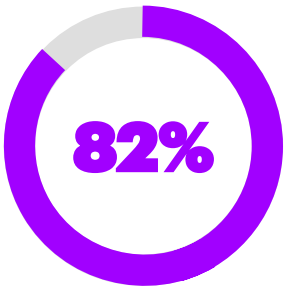
汽车制造商需要将注意力转向整个供应链，确保安全措施的应用不再局限原有的壁垒。这并非新的挑战，随着开发周期不断缩短，制造商可能会在安全措施方面走一些捷径。汽车企业需要建立安全设计文化，采用安全开发生命周期，在保证效率的同时，把安全流程嵌入到运营的所有阶段。许多领先的汽车制造商开始寻求能够提供最新安全套接层（SSL）证书的合作伙伴，以证明他们对安全性的重视程度。供应商开始更多地与具备安全管理能力的伙伴开展合作，以满足这些规范要求。这些举措将影响汽车行业和其他工业领域的前进步伐。

从以产品为导向转向以客户为中心的业务

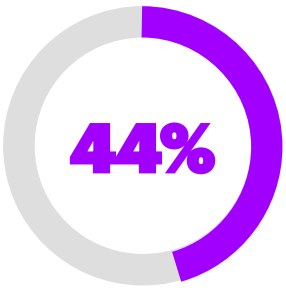
在新技术和客户期望的推动下，汽车制造商需要重新审视自己所销售的产品和销售方式。汽车制造商应优先解决客户体验的问题，远胜于闭门造车。对于呈指数级增长的数据管理，其重要程度不亚于企业不间断的运营。企业的监管需求正在得到满足，而信任和透明度问题却仍备受关注，亟待解决。云迁移和数字化转型会带来海量数据可供管理和利用。

随着车企从车辆生产者（主要价值来自车辆销售、金融服务和售后服务）转型成为以消费者为中心的出行服务商（主要价值来自出行服务、互联服务、娱乐和汽车共享计划），他们需要对客户数据提供更有力的保护。

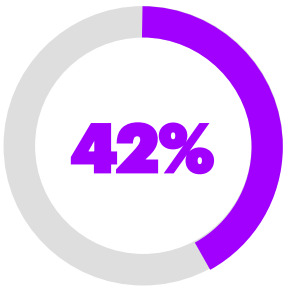
欧盟于2018年5月推出的《通用数据保护法规（GDPR）》以及其他新兴区域的隐私法规，如《加州消费者隐私法案（CCPA）》，对车企保护数据提出了重大要求。数据驱动型商业模式开辟了新的数字渠道，可以收集符合GDPR保护要求的许多不同类别的信息，包括数字标识符，如IP地址、驱动程序上的个人数据、以及车辆位置或速度等远程信息。了解哪些是敏感或私人数据会有一定难度，且对授权数据使用方面有非常严苛的限制，企业必须执行规范的流程确保这些限制得以实施。数据处理过程需要有完整的记录；一旦出现数据泄露，必须在72小时内向监管报告，这在实际操作中可能会存在一定的难度。建立新的运营控制措施，管理包括供应商和经销商等第三方披露敏感数据的风险。这些要求再加上因违规行为可能面临的巨额罚款，意味着保障安全对整个业务至关重要。



汽车业高管相信，他们能够保护数据隐私并遵守GDPR。



受访者认为，保护客户信息是其网络安全战略的一部分。



受访者表示他们有在保护企业信息。

加速创造价值

毫无疑问，汽车行业正面临双重威胁，一方面来自网络攻击，而另一方面是其运营和竞争方式的核心正在发生颠覆性改变。首席信息安全官应该及时调整自己的角色，满怀信心推进工作，助力业务加速为客户提供价值。方法如下:

01 解决安全的基础问题

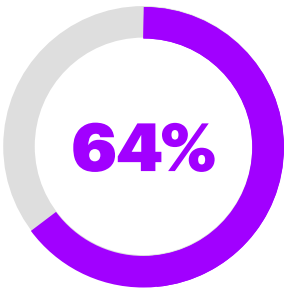
加强并保护包括IT和OT环境在内的整个价值链中的核心资产，对网络弹性不断进行压力测试，以应对当前的威胁；同时关注未来，通过使用突破性技术、智能和数据进行自动防御，积极应对未来可能的威胁。

02 将安全性扩展到更广泛的生态系统

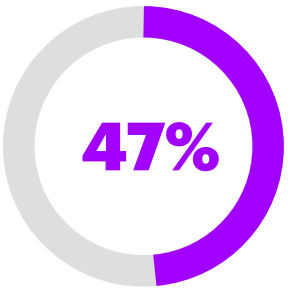
汽车制造商依赖日益复杂的合作伙伴生态系统，因此需要识别第三方供应商，制造商和经销商之间的薄弱环节和风险最大的领域，并采用适当的安全控制和治理。这样方能支持整个供应商生态系统，能够在更广阔的生态系统中维持高标准的强制性安全控制。

03 打造安全设计文化

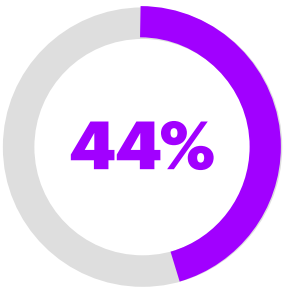
重新思考您现有的安全措施和首席信息安全官角色。安全措施需要构建在围绕汽车安全的既定生产环境之上；而新一代首席信息安全官需要具备娴熟的技术和业务能力，能够推动打造一个关注网络安全的文化。



汽车业高管要求其合作伙伴，遵守与其业务相同或更高的网络安全标准，并定期进行审核。



受访者认识到，他们需要加强网络安全监控。



受访者认为企业需要提升网络威胁分析，这是安全计划的“基础”。

作者

Uwe Kissmann
埃森哲安全服务网络安全服务
董事总经理
uwe.kissmann@accenture.com

Axel Schmidt
埃森哲全球汽车业主管
董事总经理
axel.schmidt@accenture.com

鸣谢

Eliel Mulumba
埃森哲安全服务安全专家
eliel.mulumba@accenture.com

业务联系

沈军
john.jun.shen@accenture.com

王华
ben.h.wang@accenture.com

关于埃森哲

埃森哲公司注册成立于爱尔兰，是一家全球领先的专业服务公司，为客户提供战略、咨询、数字、技术和运营服务及解决方案。我们立足商业与技术的前沿，业务涵盖40多个行业，以及企业日常运营部门的各个职能。凭借独特的业内经验与专业技能，以及翘楚全球的交付网络，我们帮助客户提升绩效，并为利益相关方持续创造价值。埃森哲是《财富》全球500强企业之一，目前拥有约47.7万名员工，服务于120多个国家的客户。我们致力驱动创新，从而改善人们工作和生活的方式。

埃森哲在大中华区开展业务30年，拥有一支1.5万人的员工队伍，分布于多个城市，包括北京、上海、大连、成都、广州、深圳、香港和台北。作为可信赖的数字化转型卓越伙伴，我们正在更创新地参与商业和技术生态圈的建设，帮助中国企业和政府把握数字化力量，通过制定战略、优化流程、集成系统、部署云计算等实现转型，提升全球竞争力，从而立足中国、赢在全球。

详细信息，敬请访问埃森哲公司主页www.accenture.com以及埃森哲大中华区主页www.accenture.cn。

说明

除非另有说明，本文所引用的统计数据代表了汽车行业受访者在调查报告《迎头赶上攻击者：2018年网络弹性状况》中的观点，埃森哲。

参考资料

1 《NotPetya不为人知的故事：网络历史上最具破坏性的攻击事件》，Wired，2018年8月22日。
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

2 https://www.accenture.com/us-en/insight-manufacturing-the-future

3 《2018网络威胁范围报告，年中网络安全风险审评》，埃森哲。
https://www.accenture.com/gb-en/insights/security/cyber-threatscape-report-2018