
A close-up, low-angle shot of a spiral staircase with a metallic finish. The stairs curve upwards, creating a strong sense of depth and movement. The lighting is dramatic, with highlights on the edges of the steps and shadows in the recesses. A bright yellow rectangular box is superimposed on the left side of the image, containing the main title in black Chinese characters.

数字化转型中，车企 如何应对网络安全与 隐私风险



从近年来中国乃至国际颁布的各种网络安全相关法规条例可知，网络安全的重要性早已上升到国家战略层面。汽车企业如何在严格的网络安全监管下合规运营本地与跨国业务，如何在数字化转型和扩展新业态服务过程中保障网络安全，如何在经营合作过程中保障数字资产、数据、云、设备、系统、网络的安全性，这些都是当下需要关注的重中之重。

数据安全是国家安全与经济社会发展重大议题

2020年4月，国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，数据被纳入生产要素的范围。6月28日，第十三届全国人大常委会第二十次会议初次审议了《中华人民共和国数据安全法（草案）》（以下简称《数据安全法（草案）》）。7月3日，《数据安全法（草案）》在中国人大网公布，面向社会征求意见，数据安全已成为事关国家安全与经济社会发展的重大议题。法律法规的日益加强和完善，对于正在数字化营销、柔性制造等推进数字化转型的汽车行业提出了更高要求，需要格外重视网络安全和隐私风险，为数字化转型之路保驾护航。

数字化转型和新业务发展带来的风险挑战



挑战一



挑战二



挑战三



挑战四



挑战五



挑战六

数字化转型带来的新风险应对

随着人们对信息技术的需求不断增强，如互联网、大数据、云计算等数字化技术在汽车这一传统工业门类加速跨界融合。特别在人工智能技术推动的“智能+”新趋势下，消费者对定制化产品的需求，促使汽车企业充分利用个人数据对设计及销售过程进行数字化改造。普华永道总结了以个人数据为驱动的新技术在运用过程面临的风险：

1. 数字化应用

汽车数字化门店主要以购车的数字化模拟以及维修保养的预约和运营业务为主。受2020年新冠疫情肆虐及直播平台销售火爆的影响，越来越多的汽车商家将购车平台搬到线上模拟平台。数字平台面对的问题包括：对DDoS/CC攻击及被攻击者敲诈勒索；不同直播平台因类似架构而暴露漏洞，导致用户信息盗取与欺诈；黑客利用修改充值金额漏洞、规避交易限制漏洞、修改用户会话漏洞等对销售过程进行破坏，这些均是数字化门店需要防范的问题。

2. 智能交通

社会智能化、网联化、共享化的发展，极大推动了“互联网+”便捷交通的发展。近年来不断涌入的创新业态：智能驾驶、移动支付、共享出行、智能交通体系等推动着智能交通产业快速发展。相较于智能交通产业整体的快速发展，网络安全风险正在不断扩散，智能交通领域聚合了海量的高价值用户数据，且由于智能交通产业链的复杂、各类应用和系统架构的异构性，各方面因素导致智能交通面临的威胁剧增。黑客攻击、安全漏洞、汽车破解劫持等问题频繁出现。

3. 精准营销

为了支持汽车销售和维护服务，诸多汽车论坛与数据分析机构对汽车用户及潜在消费者在平台或线下录入的个人信息进行用户画像分析，开展精准营销。在用户行为信息收集阶段，企业或未经用户明确同意或可预期的前提下进行信息收集；在信息的汇聚融合与用户画像阶段，企业对承担相应的数据信息安全保障义务定义不明；在信息利用与个性化推荐、营销阶段，企业需要依据用户画像、数据建模分析，根据营销策略开展营销活动形式包括广告投放、个性化推荐、服务推送等。企业利用用户敏感信息进行直接推送引起客户反感，会引起隐私保护的风险。

4. 移动业务安全

随着汽车行业线上线下结合，车企对移动应用的使用愈发频繁，开发整合新功能且与车联网更加紧密联动的应用，进入了白热化竞争。目前，超范围采集用户信息、SDK的权限和行为监管难以界定，大量应用的隐私政策缺失或不规范是当前车企开展移动业务的常见问题。

普华永道协助车企在数字化转型过程中，提供安全战略指导，设计顶层网络安全与数据保护框架，优化网络安全与数据保护组织、管理、技术，协助企业建立投资保障、人才建设、运营及治理、技术防护的安全保障体系。

挑战一

挑战二

挑战三

挑战四

挑战五

挑战六

车联网带来的新风险应对

近期国家颁布了多项方案，将发展车联网提到了国家创新战略层面。同时，人工智能和大数据分析等技术的发展使车载互联网更加实用。未来，依托人工智能、语音识别和大数据等技术的发展，车联网将与移动互联网结合，为用户提供更具个性化的定制服务。

随着车联网技术的普及与应用，随之而来的车联网安全风险日益受到关注。车联网通常采用云管端架构，包括“两端一云”。“两端”指智能联网汽车和移动智能终端，“一云”指云服务平台。其中主要面临四个风险：

• 云服务平台：

云服务平台的平台层、系统层可能存在漏洞；云服务平台也可能存在未设置访问控制策略的风险；另外由于使用公网传输，数据传输的安全性也会存在风险。

• 智能联网汽车：

智能联网汽车中会使用T-box、OBD、CAN-BUS总线、ECU、传感器、多功能车钥匙等部件，可能存在访问控制、非法启动、芯片漏洞、无身份认证、无硬件加密方式、通信未隔离以及远程升级漏洞等问题。

• 移动智能终端：

当前车联网系统通常配备移动APP来提升用户体验。可能存在破解通信密钥、分析通信协议，并结合车联网的远程控制功能干扰用户使用的风险，对车主的生命和财产安全造成威胁。

• 网络和数据：

车端与云端、车端与用户端及车内的通信同样存在被攻击的风险，例如基于伪基站的无线通信劫持、DNS欺骗的中间人攻击等。

普华永道拥有全球化的先进经验和技術，成熟的车联网安全防护体系建设与实施方法论，协助车企搭建车联网网络安全防护体系，包括信息安全管理建设、数据安全保护、云安全、智能终端安全建设、移动应用安全建设、网络安全人才培养建设等。

严格的网络安全监管下合规运营企业

挑战一

挑战二

挑战三

挑战四

挑战五

挑战六

隐私保护合规风险应对

随着法律法规相继出台，公民在隐私数据保护方面的意识逐步提高，国内外信息安全事件、监管惩罚案例频发。大数据时代车企针对隐私数据保护工作面临着严峻的挑战。

个人信息保护的全生命周期都存在隐私保护的风险：

- 在收集阶段，车企的DMS、CRM系统中保存超过千万级别的顾客个人信息，类别包括保有客户、潜在客户，收集方式包括直接收集、间接收集，随着数字化转型和业务升级，收集的个人信息类别还可能包括生物识别信息。其中，如何获取顾客收集个人信息及敏感信息的授权和明示同意，如何避免多次向顾客获取授权而影响业务，对于间接获取的顾客信息如何确保收集的合法性及正当性等都可能存在风险问题。
- 在保存及传输阶段，车企通常尚未对敏感信息分开保存，未对敏感信息进行去标识化处理，个人敏感信息传输过程中未进行加密，对个人信息安全造成影响。
- 在使用阶段，对于散落于企业内部不同系统间的个人信息，车企尚未建立有效的访问控制措施，在前端界面展示个人信息时（如呼叫中心接线员前端展

示界面）未对敏感信息进行展示限制，在数据分析平台中可能涉及用户画像、个性化展示，可能未能满足国标要求，存在未获取同意、定向推送未向用户提供选择权利等问题。在顾客权利方面，部分车企未向顾客提供个人信息查询、更正、删除等权利，未明确响应顾客请求的时限。在委托处理、信息共享方面，由于业务特性，会涉及大量第三方公司，如垂直媒体公司、广告商、数据服务商等，车企普遍和第三方公司签署了合同及保密协议，但条款颗粒度较粗，未明确说明双方在个人信息保护方面的责任和义务，也未明确双方的安全控制措施要求，无法对第三方公司进行强有力约束。在个人信息管理体制方面，很多车企未设置专职人员或岗位开展隐私管理工作，网络安全和隐私管理工作在人力资源方面存在不足。

普华永道结合国内外隐私监管的要求，形成一套成熟的隐私保护方法论，结合汽车行业的特点，协助企业从法律、管理、技术多个维度开展隐私数据保护工作，确保在复杂多变的网络环境及日益增强的政府监管下，隐私数据能够得到有效管理。



挑战一

挑战二

挑战三

挑战四

挑战五

挑战六

关键信息基础设施保护合规 风险应对

《网络安全法》第三十一条阐明：“关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。车企因其特殊性，CRM系统通常拥有超过千万级的个人信息、MES系统对生产管理起重大作用，此类平台具备关键信息基础设施的属性。关键信息基础设施运营者在网络安全维护方面，既要遵循网络安全等级保护制度对一般信息系统的安全要求，也要履行更加严格的增强性安全保护义务。前者包括制定内部安全管理制度和操作规程，采取预防性技术措施，监测网络运行状态并留存网络日志以及重要数据备份和加密等。后者包括对“人”的安全义务和对“系统”的安全义务两个方面。

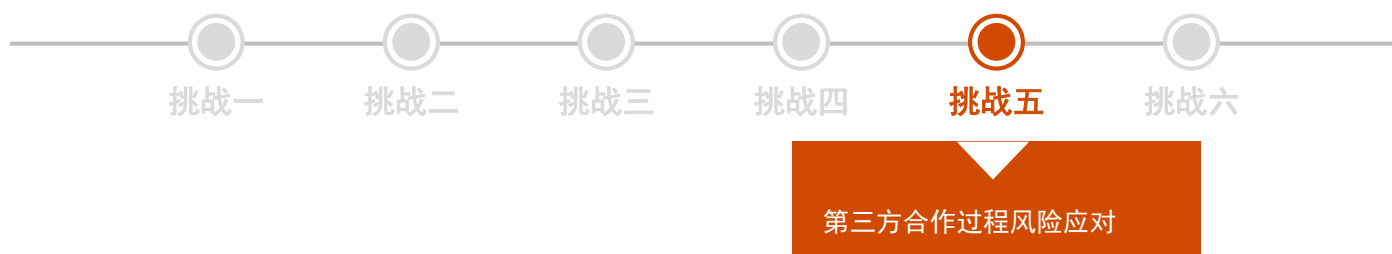
同时，车企的生产系统也需要考虑工业控制系统（ICS）安全和运营技术（OT）安全以满足最新网络安全等级保护2.0的工业控制要求。随着最近几年针对OT/ICS网络的攻击越来越普遍以及IT/OT融合的趋势，

车企需要全面评估OT环境的安全风险，从而降低关键生产系统停运的风险。

另外，为了确保关键信息基础设施供应链安全，维护国家安全，国家互联网信息办公室、国家发展改革委等12部门联合制定了《网络安全审查办法》，并于2020年6月1日起实施。违反《网络安全审查办法》，应当申报网络安全审查而没有申报的，或者使用网络安全审查未通过的产品和服务，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

普华永道协助车企识别关键信息基础设施，并结合等保、关保增强性防护要求，协助车企按照关键信息基础设施安全防护要求进行网络安全评估与改进，将最大限度避免因违反网络安全法及相关法律法规而造成的违规风险。

经营合作过程避免出现网络安全事件



汽车网络安全问题是汽车全生命周期的问题，其安全防护工作更是一个不断迭代完善的工作，需要产业链协同完成。生产制造供应链上所有参与者，从设计师、工程师到零售商和高级管理人员，都需要共同参与设计和实施汽车全生命周期安全。

汽车行业的供应链通常需要投入大量的人工来处理供应产品的来源及物流进展，而这些数据一般由供应商自主管理。各供应商的IT系统差别很大，系统之间缺乏协调和沟通。车企需要投入大量的人力物力来确保供应链数据的准确性。跨行业的解决方案与合作机制将允许所有相关合作方更紧密地连接和协调业务流程。

普华永道识别车企第三方合作范围，按照不同的业务类型制定评估内容，分析车企在与第三方合作过程中在网络安全、隐私保护、业务合作等层面的安全风险等，对风险进行归因分析，结合企业特点制定可落地的法务、管理与技术解决方案，并协助企业建立持续改进机制。





挑战一

挑战二

挑战三

挑战四

挑战五

挑战六

经销商合作过程风险应对

经销商通常代表车企面向顾客提供车辆的整车销售、零配件、售后服务及信息反馈工作。近年来经销商个人信息泄露等网络安全事件频频发生，对车企造成商誉损失，车企也可能因此遭受监管机构惩罚。

经销商的业务活动中包括对保有客户及潜在客户个人信息的收集活动，例如销售环节为车主提供试乘试驾服务，开展车展等市场营销活动等，从垂直媒体获取销售线索，主动致电招揽客户。在售后环节，除为车主提供车辆维修外，车主的车辆信息、维保记录、故障诊断信息等会被经销商进行收集记录。IT系统方面，经销商除车企要求统一使用的DMS（经销商管理系统）之外，由于经销商为独立的法人实体，也可能使用经销商自己的IT系统。经销商除内部员工外，在业务活动中也会涉及第三方人员接触到隐私数据，如保险、金融机构、活动服务商（车展）等。

普华永道协助车企加强对经销商的管理，建立定期的监督检查机制，设立经销商网络安全及隐私保护合规基线、开展面向经销商的宣贯培训、合规检查，同时也在经销商协议中明确双方的责任义务与安全管理要求，避免因经销商网络安全事件而带给车企经济及商誉损失。

汽车行业网络安全与隐私保护

为帮助企业理解复杂的法律环境、网络安全与数据保护风险，寻求适当的合规路径，降低法律风险，普华永道团队结合在网络安全和数据保护领域的广泛实践，建立了一套成熟健全的网络安全、数据保护方法论以及知识库，希望能够对企业的合规运营有所帮助。普华永道认为，成功的网络安全与隐私保护，需要注重组织、流程、技术、人员等四个方面。

1. 建立健全的网络安全与隐私保护组织体系

企业应提高网络安全意识，明确网络安全与数据保护组织，清晰定义职责，应从公司层面统筹规划网络安全与隐私保护规划建设，施行逐级分工管理。网络安全与隐私保护要考虑同步规划、建设、实施，实现安全合规、管理与安全技术并举。在管理、技术、人员岗位和操作实施层面均要符合国家法律法规、行业最佳实践要求，不断提升企业网络安全与隐私保护能力。

2. 构建网络安全与隐私保护管理体系

企业应建立、健全网络安全与隐私保护的管理体系，明确管理规章制度。落实网络安全与隐私保护相关国家法律法规，有效防范、控制和防御网络风险，规避隐私保护合规风险。增强企业网络安全/隐

私保护预警能力，增强企业业务连续性管理和灾难恢复、数据合规保护能力，提升企业的网络安全与隐私保护水平，以便支撑企业业务发展目标。

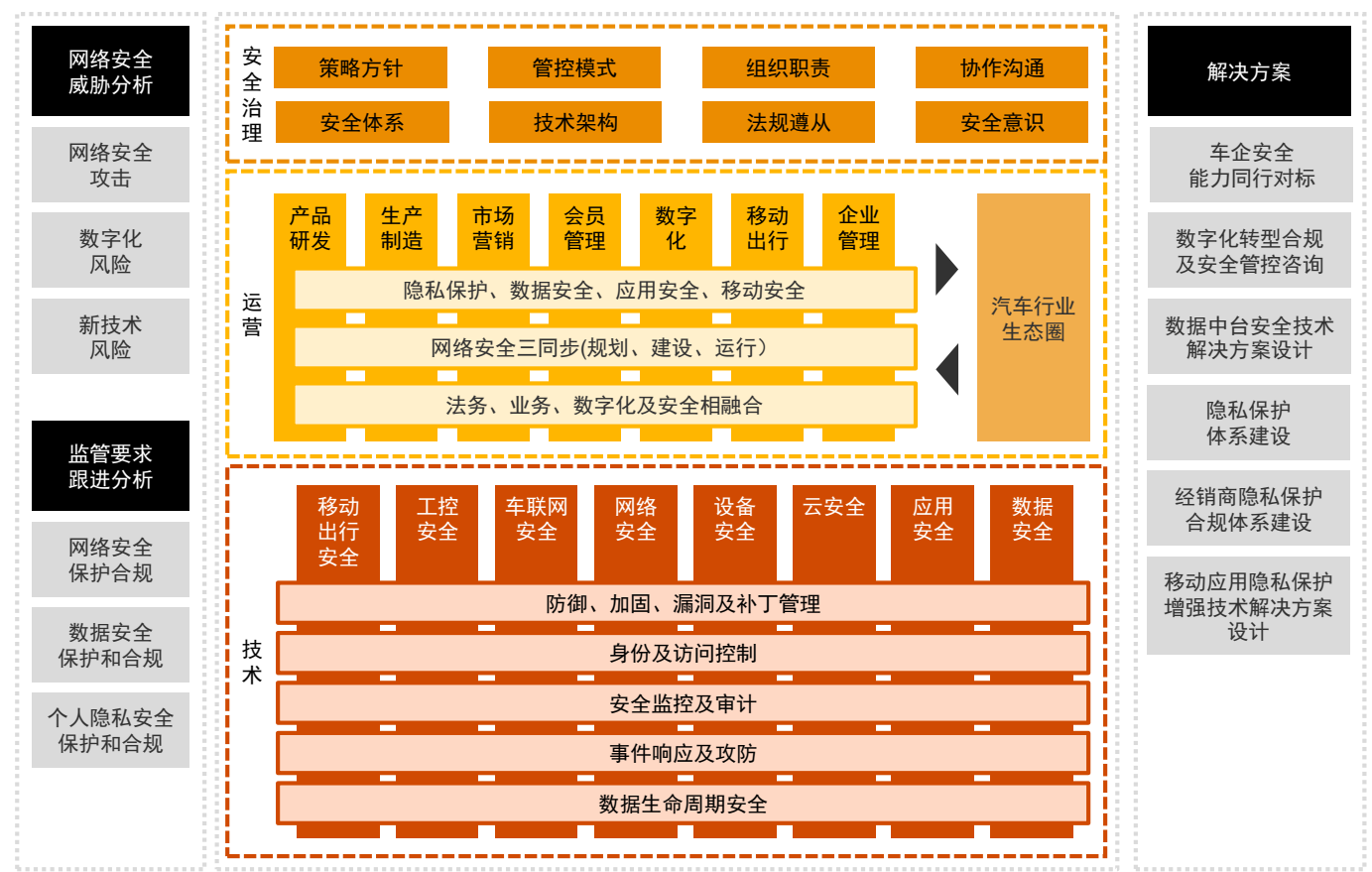
3. 加强新型技术工具的引用，推动基础创新

企业应结合业务发展目标，探索与应用新型网络安全与隐私保护技术工具。建设企业自动化威胁分析与应对平台，形成企业全方位应对网络安全与隐私保护风险的技术推动力。建设车联网安全管控平台，利用物联网、AI技术将各类型数据结合加密算法、访问控制、完整性检查、数字签名进行综合分析管控。

4. 建立网络安全与数据保护人才搭建体系，注重人员培养

企业应构建健全的网络安全与数据保护人才搭建体系，建立专业的合规、管理、技术支撑团队，明确人员培养、激励机制，团队应具备专业技能，企业内部应按领域不同进行相应的职责划分，并且在团队内部落实岗位责任和考核机制，鼓励团队成员参加国内、国际相关网络安全与隐私保护的资质认证。

汽车行业网络安全及合规管理框架



普华永道综合国际和国内相关框架模型以及汽车行业的最佳实践后，提出一套适用于汽车行业易于落地的网络安全与隐私保护方法论，协助企业构建健全的网络安全与隐私保护体系，通过网络安全威胁分析、合规风险识别、现状评估、监管要求跟进分析、同行对标和相关标准参考形成适用于不同车企的安全风险模型，针对风险提出可落地的安全合规解决方案及建议，帮助用户创建一个安全及可信的市场环境。



联系我们

金军

普华永道中国汽车行业主管合伙人

电话: +86 (21) 2323 3263

邮箱: jun.jin@cn.pwc.com

李扬

普华永道中国网络安全管理咨询合伙人

电话: +86 (10) 6533 7800

邮箱: dennis.y.li@cn.pwc.com

潘晓鸥

普华永道中国网络安全管理咨询总监

电话: +86 (21) 23232693

邮箱: sean.pan@cn.pwc.com

包红霞

普华永道中国网络安全管理咨询高级经理

电话: +86 (10) 6533 7958

邮箱: alice.h.bao@cn.pwc.com