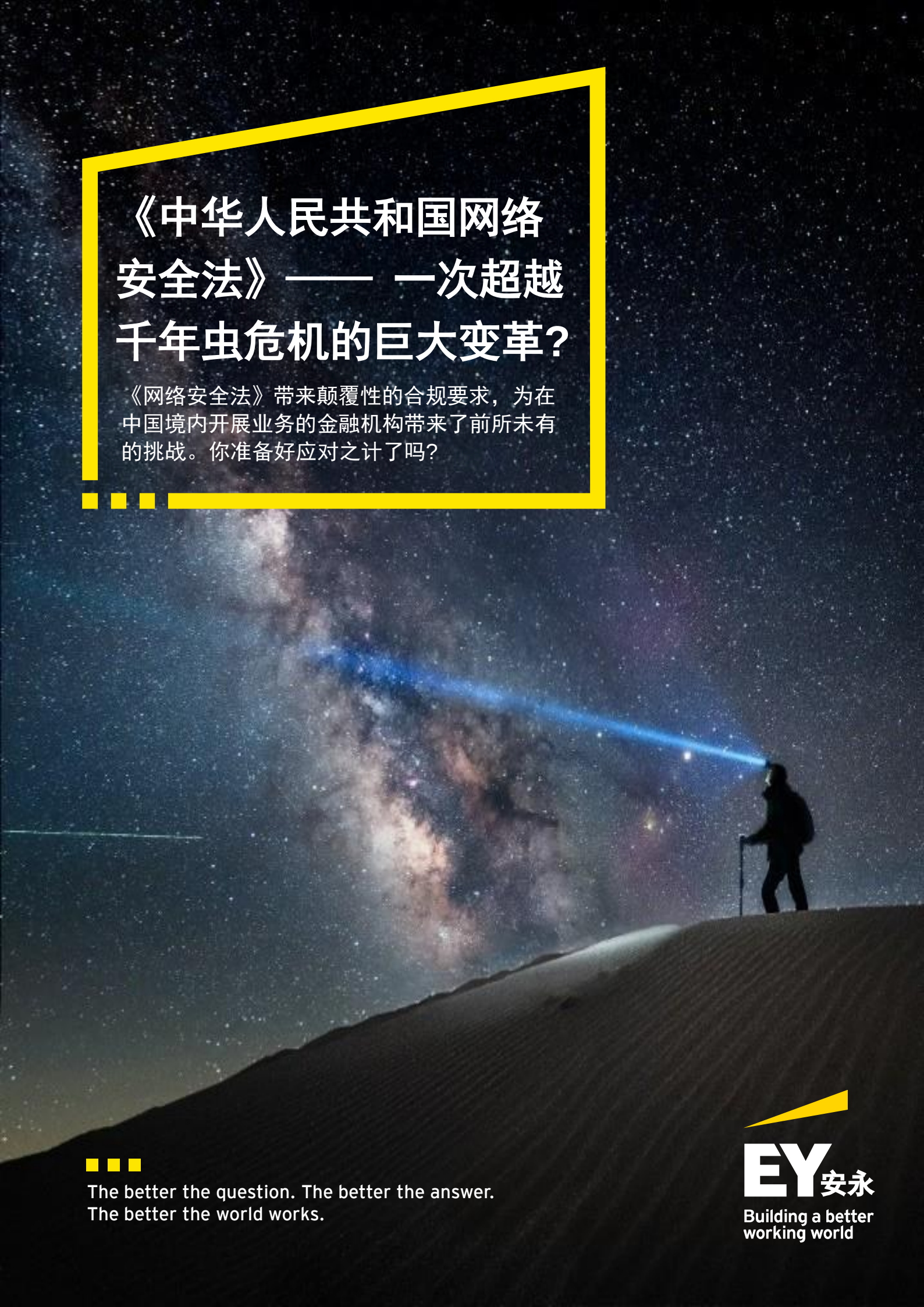


《中华人民共和国网络安全法》—— 一次超越千年虫危机的巨大变革?

《网络安全法》带来颠覆性的合规要求，为在中国境内开展业务的金融机构带来了前所未有的挑战。你准备好应对之计了吗?

The better the question. The better the answer.
The better the world works.

EY 安永
Building a better working world

《中华人民共和国网络安全法》（以下简称《网络安全法》）是中国首部针对网络隐私和网络空间安全管理制定的综合性监管法案。该法案的实施促使所有在中国境内开展业务的金融机构必须采取全面的响应措施。上一次出现类似情形还要追溯到上世纪90年代末，各大企业都在不遗余力地升级计算机和应用程序以抵御“千年虫危机”。

为应对“千年虫危机”，全球共耗资3,000亿美元。尽管人们认为这仅是一起单一的孤立事件，不会再次发生，但《网络安全法》的出台却给人以似曾相识之感。

为确保公司及核心供应链在《网络安全法》框架下的合规运营，在中国境内开展业务的外资金融机构和业务范围覆盖海外市场的中资金融机构都必须启动对企业计算机系统的全面技术评估，所需费用和时间成本令人关注。

《网络安全法》对金融机构将产生哪些直接影响？

影响规模和范围

不同于旨在限制外部信息输入中国境内的“防火墙”，《网络安全法》的主要目的在于防止数据流出境外。虽然该法案仍在不断演进和完善当中，但已经明确的适用对象包括关键信息基础设施运营者，其中无疑涵盖金融机构。

连同其他已经实施或仍在拟定当中的法律法规和行业标准，《网络安全法》明确了金融机构的一系列新的义务和责任。

除了类似《一般数据保护条例》（GDPR）的隐私保护条款，《网络安全法》不断丰富和完善的措施、准则及合规要求对在中国境内开展业务的金融机构意味着：

遵守《网络安全法》为何具有挑战性？

了解中国网络安全监管方法

《网络安全法》的出台反映了全球范围内加强网络空间安全监管和打击对公共安全存在威胁的网络行为的广泛趋势。该法案实施的目的之一在于让中国与全球网络安全最佳实践接轨，但其实际影响远不止于此。《网络安全法》还旨在对中国境内产生的数据和内容行使司法管辖权——坚定主张“中华人民共和国境内的互联网属于中国主权管辖范围”。

这意味着《网络安全法》具有中国特色，需要大多数西方企业花时间逐步理解。《网络安全法》合规要求金融机构必须从根本上转变在中国境内收集、储存、传输和使用数据的方式方法。例如，该法案：

引入了新的数据类别

《网络安全法》重点关注在中国境内所生成信息的流动性质，不仅强调“个人信息”，同样涉及“重要数据”——这对于西方企业而言是一个新的数据类别。任何与国家安全、经济发展或社会公共利益相关的信息都被视为“重要数据”。

对不同行业而言，“重要数据”的内涵可能存在差异。针对金融机构，“重要数据”涉及可能对宏观经济产生实质性影响的业务交易数据。然而在中国，“重要信息”的定义和构成可由相关监管机构依具体情况决定。

引入了数据本地化要求

金融机构在中国境内运营时收集和产生的“个人信息”和“重要数据”必须在境内存储。因业务要求需向境外提供的，必须通过政府相关部门的安全评估。为规避风险，目前有向海外总部传输数据需求的金融机构必须重构其数据传输机制，引入必要的安全评估流程。安全评估的具体标准仍在制定当中。

提出了严格且广泛的规定

《网络安全法》的适用范围涵盖信息安全、通信安全、计算机安全、自动化和控制系统安全。具体要求更是细化至网络硬件层面。某些网络设备和网络安全产品必须通过安全认证以确保符合国家相关标准。

中国的立法和执法风格也增加了合规难度，即该法案内容以中文撰写、采用原则基础法并且在应用过程中需要运用判断。这也就导致了《网络安全法》的应用对于西方企业而言可能比较复杂并容易引起误解。

调整运营模式，遵守中国《网络安全法》

对新合规要求采取适当应对措施

依据现有网络安全的成熟度，为实现《网络安全法》合规，大多数金融机构需：：

1 强化网络安全

现有网络安全设备无法达到该法案要求的网络安全规范等级。机构须采取统筹协调方法，以：

a. 在应用程序和网络架构层面安置适当的“关口和监控”

b. 精简并标准化技术堆栈

c. 集中数据包流，以确保完整性和透明度

d. 利用安全编排、自动化和响应（SOAR）工具，集中处理所有安全日志，诊断实际威胁并迅速响应

e. 创建面向业务的记分卡，以便业务管理人员能够直观认知网络威胁和攻击

2 引入内容安全

机构须启动其网络内的信息监控以识别受限内容。所有文本、音频及视频内容都需要进行审查以甄别被认为不当内容。违规内容必须被删除、记录并通报。对于以电话录音形式记录其经纪人与客户通话的金融机构而言，这项规定已经带来了巨大挑战。

3 建立新的安全审核机制

机构必须定期审查其网络技术系统和流程，其中包括应急响应协议。《网络安全法》对大多数网络安全实践中超出标准事件响应能力的应急响应措施都作出了具体要求。

4 保护个人信息

机构在收集客户信息前须明示并征得客户同意，告知客户其信息用途，在发生数据泄露事件时通知政府相关机构，并且有义务应客户要求删除或修改其个人数据。

5 尽可能减少跨境数据传输活动

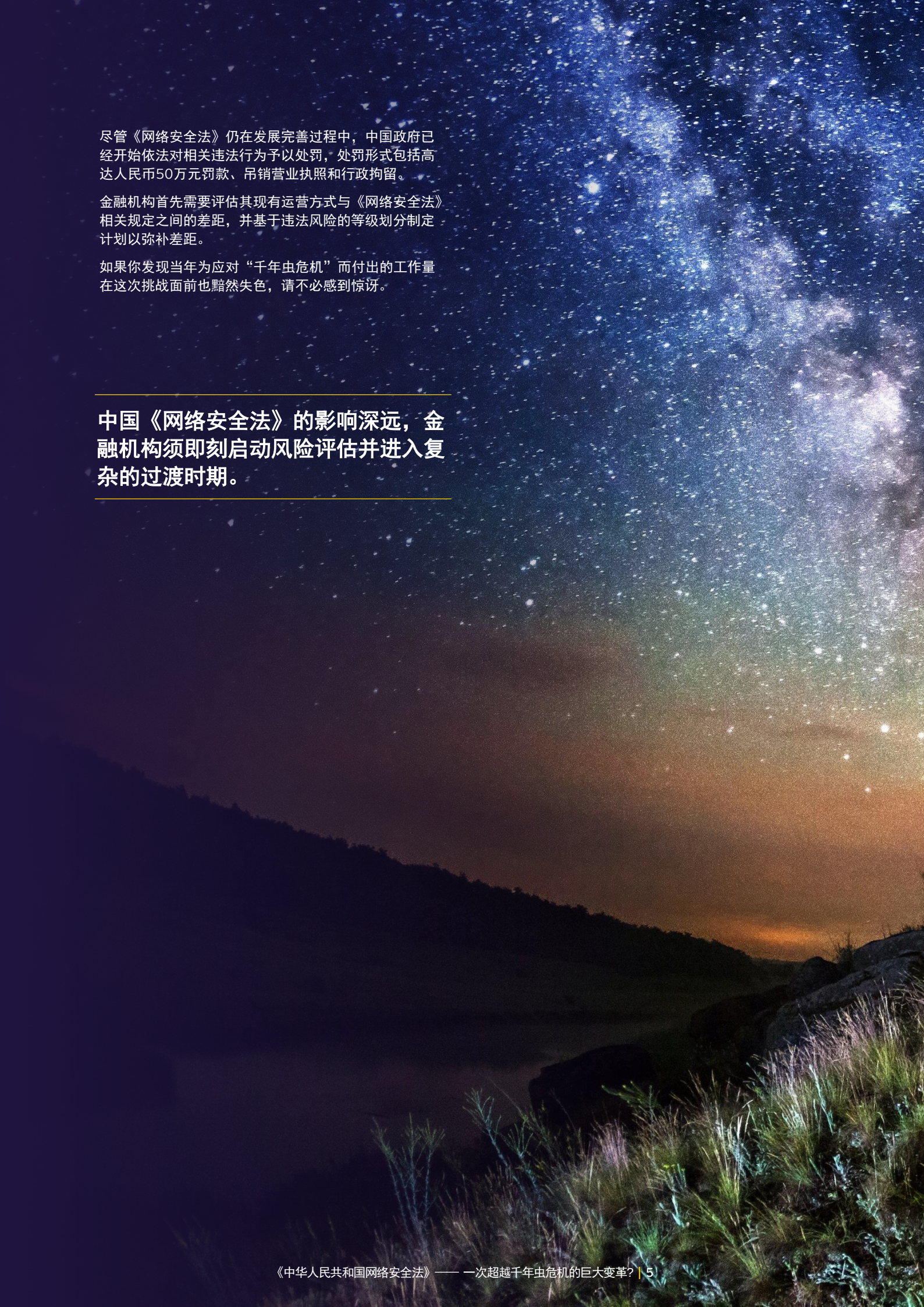
拥有集中式客户关系管理（CRM）、人力资源（HR）、采购或其他关键业务系统的跨国公司需要针对其流向共享服务中心的数据制定专门策略。一些金融机构已经开始考虑在本地建立数据中心，或转而使用有中国境内数据中心托管的云服务。

尽管《网络安全法》仍在发展完善过程中，中国政府已经开始依法对相关违法行为予以处罚，处罚形式包括高达人民币50万元罚款、吊销营业执照和行政拘留。

金融机构首先需要评估其现有运营方式与《网络安全法》相关规定之间的差距，并基于违法风险的等级划分制定计划以弥补差距。

如果你发现当年为应对“千年虫危机”而付出的工作量在这次挑战面前也黯然失色，请不必感到惊讶。

中国《网络安全法》的影响深远，金融机构须即刻启动风险评估并进入复杂的过渡时期。



联系安永

梁尚文
安永（中国）企业咨询有限公司
大中华区金融服务部
风险咨询服务
主管合伙人
+86 10 5815 3236
sherman.leung@cn.ey.com

冯哲
安永（中国）企业咨询有限公司
大中华区金融服务部
风险咨询服务合伙人
+86 21 2228 6855
wilson.z.feng@cn.ey.com

EY 安永 | Assurance 审计 | Tax 税务| Transactions 交易 | Advisory 咨询

关于安永
安永是全球领先的审计、税务、交易和咨询服务机构之一。我们的深刻洞察和优质服务有助全球各地资本市场和经济体建立信任和信心。我们致力培养杰出领导人才，通过团队协作落实我们对所有利益相关方的坚定承诺。因此，我们在为员工、客户及社会各界建设更美好的商业世界的过程中担当重要角色。

安永是指Ernst & Young Global Limited的全球组织，也可指其一家或以上的成员机构，各成员机构都是独立的法人实体。Ernst & Young Global Limited是英国一家担保有限公司，并不向客户提供服务。如欲进一步了解安永，请浏览ey.com。

APAC no. 03007806
ED None

ey.com/china

关注安永微信公众号
扫描二维码，获取最新资讯。