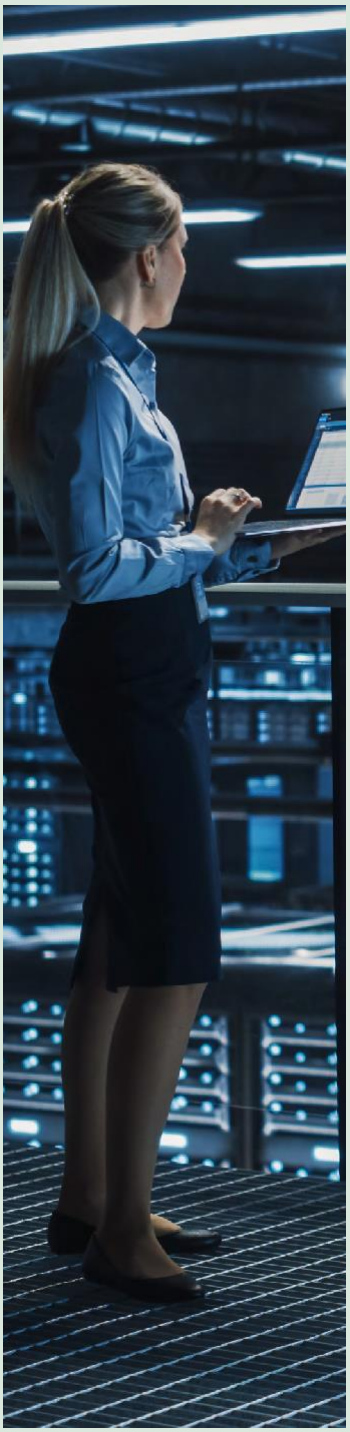
白皮书



中国企业应当如何处理好信息安全的两难处境

摘要

目前，中国各行各业的企业正在积极进行数字化转型。在这个过程中，信息安全问题带来了一个普遍的两难处境：一方面是企业自身的信息安全要求、以及国家信息安全法规的要求，另一面是用户体验、复杂性、IT及运营效率、成本、上市时间等方面的影响。如何更好地解决这个问题是企业不能回避的问题。

我们从风险角度来进行归纳，信息安全法规方面的风险包括：由于不合规而带来的战略目标的达成、业务连续性、业务转型、服务质量、商誉损失等方面的风险； 而在企业架构各个层面的安全风险则包括：业务连续性、个人和商业数据保护、客户流失、服务可用性、服务水平、商誉、变更和转型的安全性。

本文重点分析了中国企业面临的安全问题，着重介绍了各类威胁的原理、以及安全法规的要求，并从企业组织面临的特定风险和合规要求两个角度对国内企业提出了建议。

通过阅读本文，企业可以更好地了解信息安全问题，把信息安全风险的管理提升到企业架构层面，通过业务、数据、应用和技术的分析，在满足企业转型各个领域的目标的同时，以最小的代价设计、过渡及运营信息安全，并取得与运营目标之间的平衡。

Infosys®
Navigate your next

行业背景

在国内，每个企业的规模、业务环境的复杂度、面临的挑战都不同，同时，不同的企业发展也不均衡，在诸多的短期、中期、长期目标中，不得不选择出最佳的路径。

企业一方面需要降低风险，另一方面需要考量用户体验、复杂性、IT及运营效率、成本、上市时间等方面的影响。

从整体角度设计企业安全架构的需求日益增长。企业需建立正确的、全局的企业安全架构愿景和原则。

解决方案

我们建议采用企业架构设计方法来对安全架构进行整体设计。

这个方法的好处在于：**1. 安全解决方案能够明确地针对企业的目标和现状；2. 更好地在企业其他计划中的转型设计中融入安全方案，防止出现重复建设；3. 建设一个整体的安全架构视图有利于建设步骤的优化、以及变更和维护。**

那么，如何从全局层面对企业安全架构进行设计？

从全局层面进行安全架构设计是指：1. 综合考虑了企业的业务战略、业务驱动力、企业环境因素；**2. 对企业安全架构要达到的愿景进行正确的定义**；3. 在业务架构和IT架构层面逐步落地安全解决方案（参见TOGAF 9中关于架构设计方法ADM的叙述）。

显然，其中第2条，即“对企业安全架构要达到的愿景进行正确的定义”是承上启下的最核心的步骤。

以下，我们从安全法规以及企业自身安全要求两个层面进行研究，以便能够帮助企业更好地定义出正确的安全架构愿景，同时，也在解决方案层面做出相应的建议。

第一部分：法规遵从性要求及对策

中国已经建立了网络安全的基本法律合规框架，要求企业加强安全合规能力，履行自身法定合规义务，否则将可能遭受不同程度的业务损失。合规是企业安全的第一步，也是最重要的一步。

以下是三大基本法规：

1. 《中华人民共和国网络安全法》。
2. 《中华人民共和国数据安全法》。
3. 《中华人民共和国个人信息保护法》。

国家互联网信息办公室（“网信办”）等政府部门已颁布多项法规以实施“三部基本法”。此外，其他政府监管部门和相关机构，如全国信息安全标准化技术委员会（“TC260”），也发布了许多标准以提供更详细的指导。

企业的合规性涉及多个部门。企业有必要正确识别所有相关组织。

为了合规，企业需要实施网络安全等级保护、个人信息保护、风险评估、日常监测、数据跨境评估等措施。其中，网络安全等级保护和数据跨境传输在中国目前受到更多关注。

同样地，我们建议企业将信息安全的要求列入到企业架构迭代中，尤其是融入到业务和架构的原则中。此外，在进行业务、应用、数据和技术架构的设计时，应当参考以下内容：

1. 等级保护要求和实践

作为规范性文件，网络安全等级保护（简称“等保”）是指对信息系统分等级实行安全保护，对信息系统中使用的安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级进行响应、处置。

根据《网络安全法》，所有网络运营者都需要按照等保制度的要求，履行安全保护义务，包括等保定级和评估。一般来说，如果不开展等保工作就等同于违法。

等保的技术框架可概括为”一个中心、三重防护”，”一个中心“指安全管理中心，”三重防护“指安全通信网络、安全区域边界和安全计算环境。

等保包含五个级别，级别越高，要求越严格。

通常，在明确了本企业的等保要求后，便可以把等保要求纳入到架构愿景和原则中，并逐步形成解决方案。

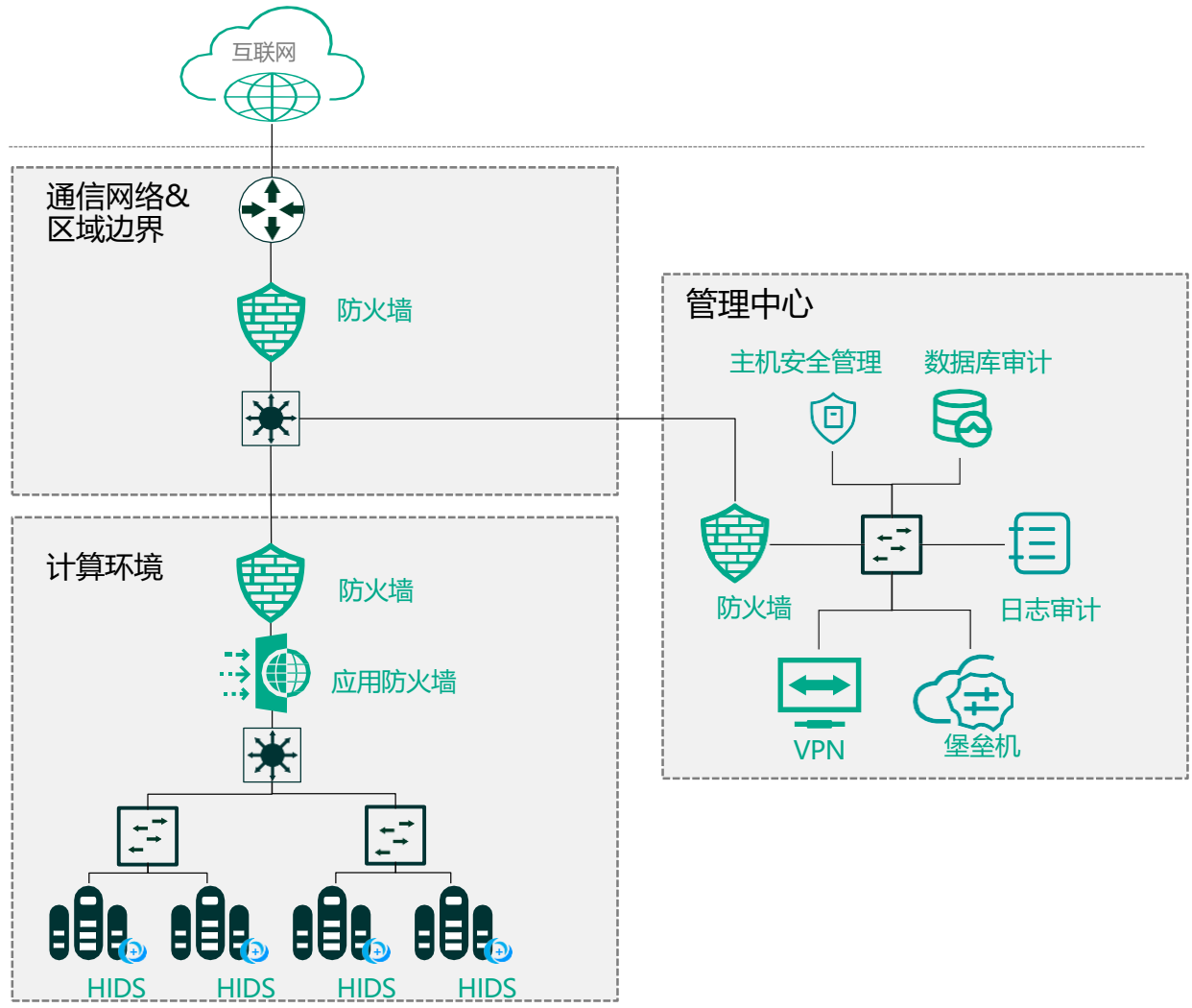
关于满足等保要求，为了以最小的成本、时间和变更得到最大程度的合规效果，我们的建议是按照以下五个步骤来实现等保:

1. 定级

企业可根据系统服务受到破坏后对侵害客体（比如公民、法人和其他组织）的侵害程度，自主确定自己信息系统的安全保护等级。由公安机关对信息系统的定级情况开展审核，并对发现定级不准确的予以纠正。

等保二级解决方案示例如下.

图1. 等保二级解决方案示例



2. **备案**

填写《信息系统安全等级保护备案表》及其他一系列材料提交至公安进行备案审核。

3. **安全建设与整改**

对系统进行梳理与调研，出具《差距性分析》和《整改方案书》等，进行整改和系统安全加固，找出不安全因素进行整改。

4. **信息安全等级测评**

整改完成之后，请测评机构进行全面测评。

5. **监督检查**

公安机关监督检查等级保护工作，颁发测评报告。

企业通过等保建设，一方面是满足合规要求，另一方面也可提升企业安全性和规范性，提升企业自身业务系统的安全性。

面向等级保护的安全技术建设，提供等保二级和等保三级的解决方案示例供参考。

等保三级解决方案示例如下。

表1. 等保二级安全产品示例

类别	内容	要求（建议）
主机安全	满足安全计算环境安全要求	必备
安全管理中心	满足安全管理中心要求	必备
防火墙	满足安全区域边界和安全通信网络的要求	必备
堡垒机	身份鉴别、操作审计 访问控制	选配
应用防火墙(WAF)	边界入侵防范，应用安全	选配
VPN	满足远程访问传输安全要求	选配

图2. 等保三级解决方案示例

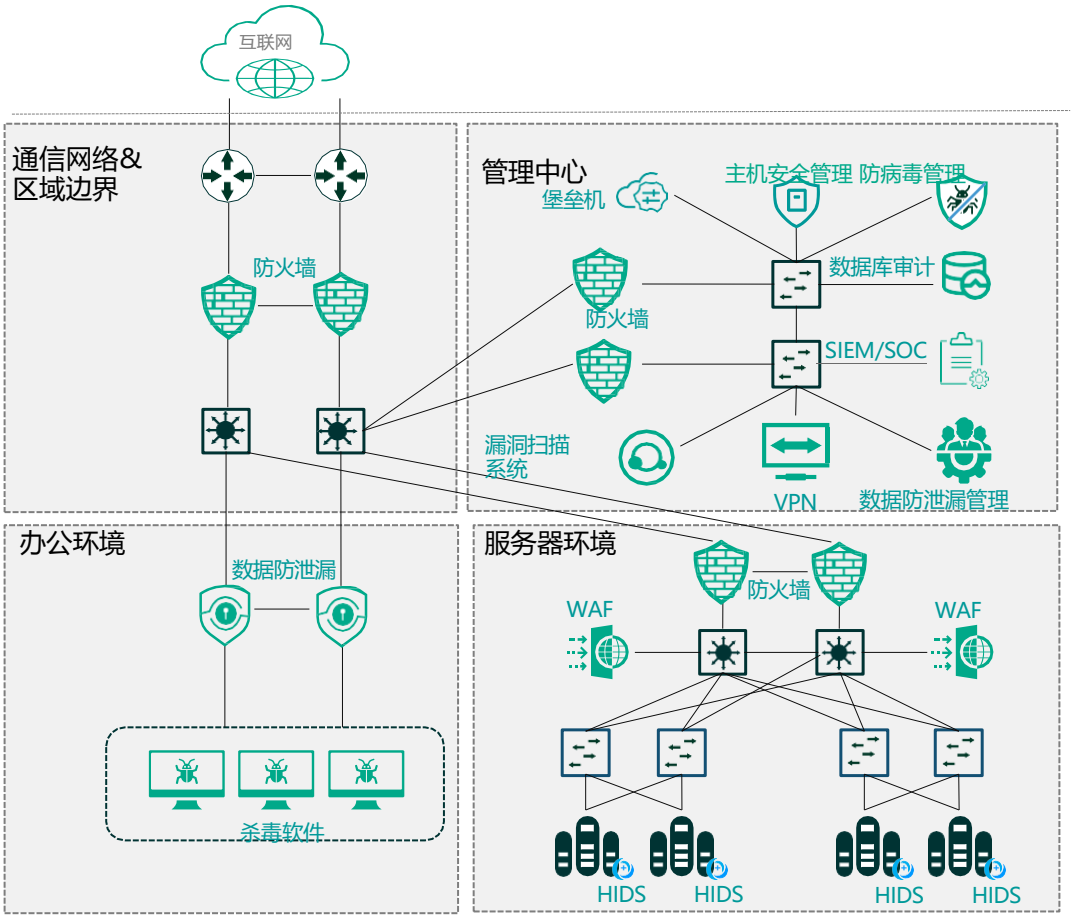
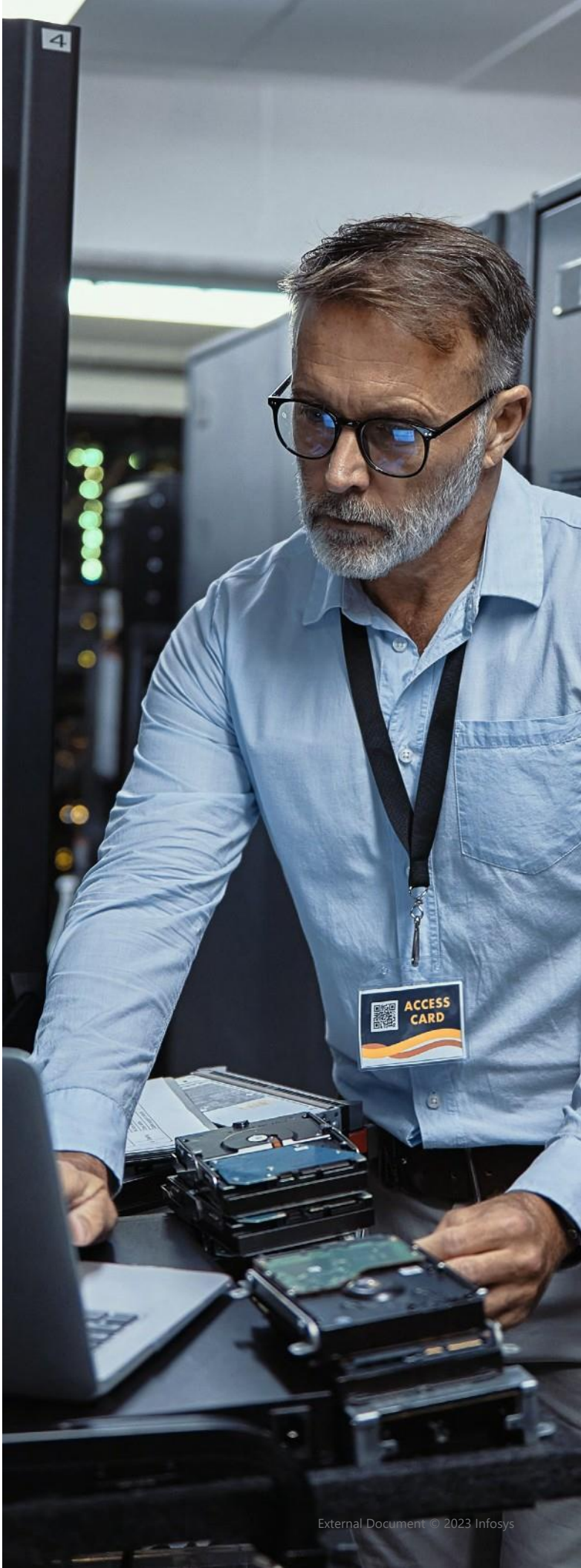


表2. 等保三级安全产品示例

类别	内容	要求（建议）
主机安全	满足安全计算环境安全要求	必备
安全管理中心	满足安全管理中心要求	必备
防火墙	满足安全区域边界和安全通信网络的要求	必备
堡垒机	身份鉴别，操作审计，访问控制	必备
应用防火墙(WAF)	边界入侵防范，应用安全	必备
漏洞扫描	发现和管理已知漏洞	必备
数据库审计	满足应用及数据安全要求	必备
VPN	满足远程访问传输安全要求	选配
DLP	数据泄露保护	选配



2. 数据跨境要求和实践

根据《数据安全法》，“数据”不仅包括电子数据，还包括以非电子形式记录或存储的数据（如纸质文件记录的数据）

“重要数据”的定义为“特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。” “个人信息”定义为“以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。” “敏感个人信息”定义为“一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。”对于敏感个人信息的保护应高于一般个人信息，也受制于更严格的出境监管。将数据处理者向境外提供在中华人民共和国境内运营中收集和产生的“重要数据”和“个人信息”视为数据出境活动。

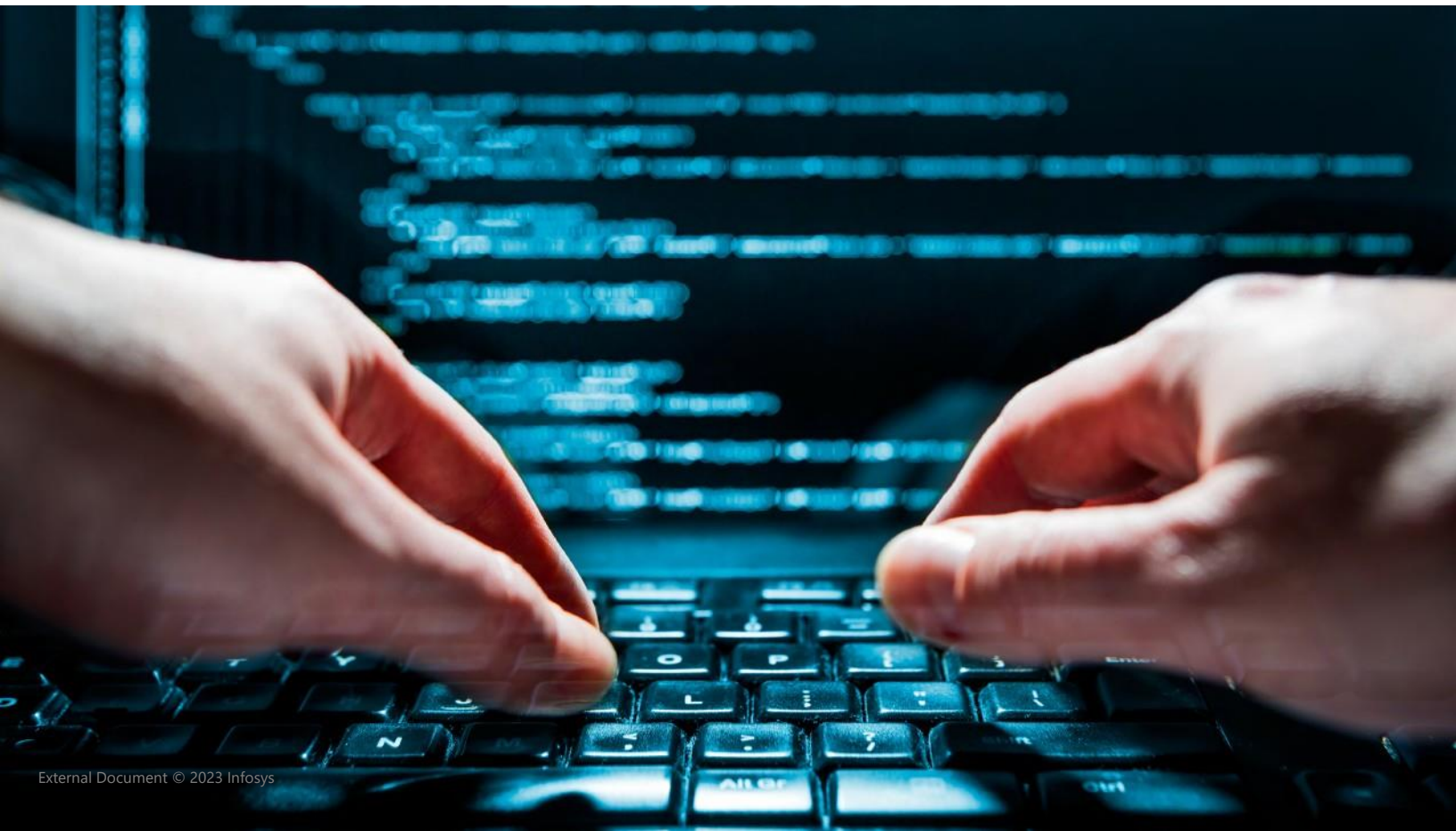
实践中，中国大多数企业一般只涉及个人信息，并不会涉及到重要数据。对于那些拥有大量个人数据（客户、合作伙伴和内部员工等）的公司，这些数据的跨境传输可能会违反三大基本法。

表3. 个人信息跨境传输三大机制

施行时间	发布单位	名称	简称
2023-6-1	国家网信办	《个人信息出境标准合同办法》	标准合同
2022-12-16	全国信息安全标准化技术委员会秘书处（TC260）	《网络安全标准实践指南—个人信息跨境处理活动安全认证规范V2.0》	安全认证
2022-9-1	国家网信办	《数据出境安全评估办法》	评估办法

因此，数据跨境传输应当确保满足如下其中之一：

1. 通过国家网信部门组织的安全评估。
2. 按照国家网信部门的规定经专业机构进行个人信息保护认证
3. 按照国家网信部门制定的标准合同与境外接收方订立合同



建议企业遵循“两步走”原则来分别定义安全架构愿景、以及提出解决方案。

第一步：确定触发场景。

企业应首先根据出境场景，识别是否需申报安全评估，如触发则应选择申报安全评估作为出境机制。

然后根据相应的场景，增加相应的愿景描述（参见TOGAF 9中“利用业务场景建立架构愿景”相关的方法描述）。

第二步：选择合适的数据跨境传输机制。

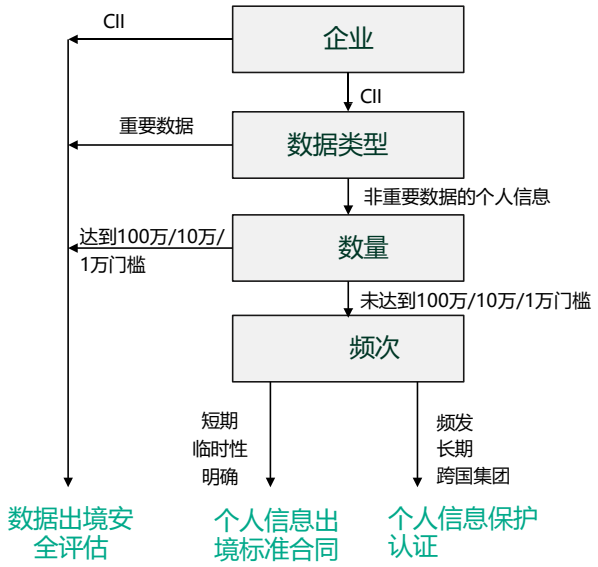
在解决方案层面，如未触发申报安全评估，企业可以根据业务活动和数据情况订立标准合同或开展安全认证。

对于个人信息的短期和临时跨境传输，或跨境交易场景明确，“标准合同”具有高效、低成本的优势。

对于集团关联公司之间的跨境传输，个人信息跨境处理更容易制定和遵循统一规则，最好使用“安全认证”。

其中“CII”指的是关键信息基础设施，“100万/10万/1万门槛”指的是处理100万人以上个人信息的数据处理者向境外提供个人信息，自上年1月1日起累计向境外提供10万人个人信息或者1万人敏感个人信息。

图3. 个人信息数据出境机制选择



第二部分：国内安全威胁的类型及对策

目前国内三种最常见的安全威胁是分布式拒绝服务攻击（简称“DDoS”）、勒索软件和数据泄露。它们的数量不断增加（例如，DDoS 现在已达到 TBPS级别）和复杂性不断增强；它们大多是利润驱动的（例如，勒索软件即服务的出现）；数据泄漏越来越受到关注，因为大多数业务职能部门、架构师和 IT 运营部门都不断看到数据泄露在其解决方案和运营中的潜在影响。

据媒体报道，单起网络安全事件可能达到数百万美元，而且这一趋势仍在上升。值得注意的是，数字化转型采用越来越多的人机交互、更多的应用程序集成、更多的数据传输和更多的迁移，在该过程中不断产生漏洞并重塑IT架构和企业使用IT工具的方式。采用的数字技术越多，威胁成为现实的机会就越大。

我们建议企业将信息安全的威胁列入到企业架构迭代当中，融入到业务和架构的原则中，在早期建立风险识别机制，并且在其业务、应用、数据和技术架构中设计具体的技术和管理的应对方法。

威胁1：分布式拒绝服务（DDoS）

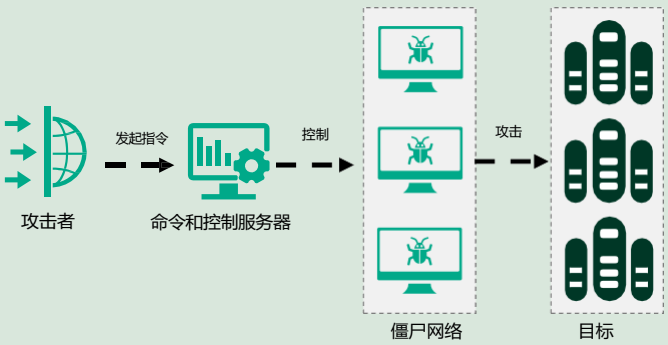
作为网络安全的严重威胁之一，DDoS已经活跃了20多年，攻击事件不仅频繁发生，并且新型攻击方式也在不断涌现。

DDoS 攻击是指不同位置的多个攻击者同时攻击一个或多个目标，攻击流量模拟正常的IP、TCP或其他流量，但由于是同时发生并且高于目标系统可以处理的能力，使得受害系统无法响应真正的业务请求，甚至用户完全得不到系统的任何响应。

完整的DDoS攻击包括四种类型的参与主体：攻击者，命令和控制服务器（“C&C”），僵尸网络和目标。攻击者主机发起攻击指令，指示C&C和僵尸网络发起DDoS攻击。C&C有助于隐藏攻击者，僵尸网络通过发送大量攻击流量直接攻击受害者。

僵尸网络由起初基于传统主机，逐渐发展为基于包括智能手机和物联网在内的各种无线设备。

图4. DDoS攻击示例



僵尸网络发起攻击的方式增加了其复杂性，其主要有两种方法：“流量攻击”主要目的是通过泛洪包裹来消耗网络带宽；“资源耗尽攻击”会耗尽主机的内存和进程（例如，通过设置大量不完整的TCP会话），导致无法提供服务。

根据《2022年上半年DDoS攻击威胁报告》分析，国内的DDoS情况如下：

- DDoS 攻击的威胁创下历史新高。2022 年上半年的攻击次数达到了四年来的最高水平，是 2021 年同期的三倍。游戏和视频行业在所有受害者行业中排名前二。
- Tb级攻击连续3个月出现，百G级攻击平均每天超40次。
- 7成攻击持续时间不超过30分钟。其中，35%的攻击时长小于5分钟。

- 当传统攻击（例如UDP反射和SYN大包）由于防御能力的增长而保持稳定时，新类型（如TCP反射和PSHACK）继续增加，因为它们更难防御。

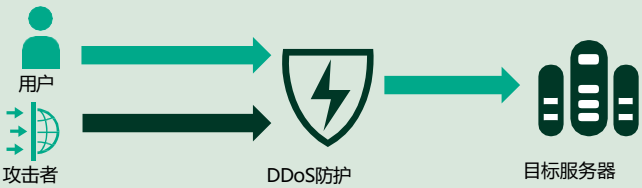
对于经常遭受DDoS攻击的企业，印孚瑟斯建议把DDoS防护的内容纳入安全架构愿景中，并在技术架构中采用以下方法。

DDoS攻击变得越来越复杂，更广泛和更便宜，需要企业采取相应的措施来进行应对。我们建议的对策包括：

- 从运营商处购买服务以绕过攻击（例如分布式集群防御，据报道称是最有效的方法）：当增加数据中心的入站和出站带宽不太可行时，可以选择利用位于上游网络的旁路服务。
- 部署 CDN：CDN可以隐藏主机的IP、将网站内容分发到多台服务器，用户就近访问CDN服务，不仅可以改善用户体验，还可以作为DDoS防护的补充方法。
- 提高路由器，交换机，防火墙等的吞吐能力。对于ISP、云运营商和其他企业来说都是如此。
- 提高服务器的安全级别：采用漏洞扫描、及时更新安全补丁、关闭未使用的服务和端口等安全措施，从而降低攻击者利用漏洞发起DDoS攻击的风险。
- 异常流量清洗：通过抗D专用设备进行异常流量清洗，保证企业的正常业务不受影响。

下图表示了 ISP和云运营商如何保护用户免受 DDoS 攻击的通常方式。

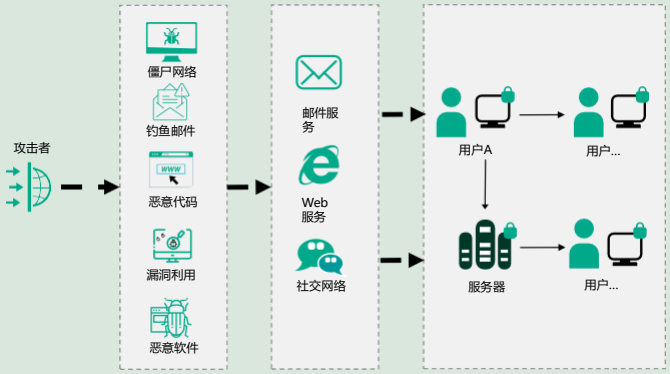
图5. DDoS防御示例



威胁2：勒索软件

勒索软件属于木马家族的成员，早在1989年便已出现。近年来，勒索软件攻击频发。

勒索病毒主要以邮件、程序木马、网页挂马等的形式进行传播。一旦系统被感染，数据就会被加密，受害者必须支付赎金才能解密数据。



勒索软件通常使用对称加密算法和非对称加密算法的组合来加密数据。理论上，如果使用暴力破解需要数百年的时间。因此，通常不可能在不知道密钥的情况下进行解密。

根据国内某安全机构分析，国内的勒索攻击态势呈现如下趋势：

- 勒索攻击已成为中国企业面临的主要网络威胁之一。
- 攻击者不断丰富他们的攻击和勒索方法。
- 各种主要系统都容易受到攻击：Windows，Linux，macOS甚至工业控制系统。
- 流行的勒索软件包括DarkSide、Conti、MacRansom、MacSpy、EKANS、Cring等。
- 黑客们正在开发多种勒索模型：“窃取+加密”，“窃取+加密+泄漏”等。
- 勒索软件攻击者开始采用高级可持续威胁攻击（简称“APT“）发起攻击。
- 勒索软件即服务（简称“RaaS”）模式愈发成熟壮大。在利益的推动下，RaaS被认为是勒索软件攻击迅速蔓延的关键原因之一。
- 勒索软件攻击者开始与数据泄露平台合作以获得更多利益。

印孚瑟斯建议把防止勒索软件内容纳入安全架构愿景中。建议采用如下应对措施：

- 定期备份重要数据。
- 及时更新系统和安全补丁。
- 端点保护。安装杀毒软件和EDR（端点检测和响应），关闭不必要的服务和端口。
- 建立网站和应用白名单。
- 提升员工安全意识。比如设置高强度密码，不要点击来源不明的邮件等。
- 制定应急响应预案。

威胁3：数据泄露

国内数据泄露频繁发生，以下是常见原因：

- 网络攻击：攻击者利用漏洞侵入目标系统以获取数据
- 内部攻击：内部人员滥用特权，有意或无意地泄露数据。
- 第三方泄漏：组织的第三方供应商在有效使用条款过期后继续使用数据。这可能是故意的，也可能是由于操作不当。
- 物理安全问题：包括未加密的移动存储设备丢失或被盗，或未受保护的数据备份。

根据《2021年数据泄露态势分析报告》，国内的数据泄露态势呈现如下趋势：

- 2021年，数据泄露占所有数据安全事件的比例为80%。大多数数据泄露都是利益驱动的。
- 统计数据显示，在数据泄露的原因中，内部人员和攻击者占的比例大致相同，其中内部人员占42%，攻击者占39%。
- 在所有数据泄露事件中，个人信息泄露比例超过60%，排名第一。
- 在个人信息泄露的行业中，互联网公司占比最高，其次是医疗和金融保险行业，合计占比达60%。

与此同时，近年来数据泄露的频率和成本迅速增长。

那么企业应该如何处理数据泄露事件呢？**印孚瑟斯建议把防止数据泄露的内容纳入安全架构愿景和原则中，并建立全面的数据安全架构治理。**

数据安全治理要求企业组织在数据安全战略的指导下，多个部门协作实施，包括建立组织数据安全治理团队，制定数据安全相关制度规范，构建数据安全技术体系，建设数据安全人才梯队等。

数据安全治理聚焦数据全生命周期，从安全管理、安全技术和安全运营三个方面构建企业数据安全体系。

1. 安全管理体系

- 组织建设。包括数据安全组织机构的架构建立、职责分配和沟通协作。建议自上而下的建立管理组织架构，确保数据安全责任层层落实。
- 制度流程。建议结合自身业务场景，在数据安全涉及的

不同领域编制一级、二级、三级、四级的管理和技术文件，指导数据安全制度体系的总体建设。

- 培训和评估。建议加强数据安全工作人员的安全意识和专业能力

2. 安全技术体系

建议采用国家标准和技术协会（简称“NIST”）网络安全框架（简称“CSF”） IPDRR模型的方法论，在数据全生命周期（包括数据收集、传输、存储、使用、共享和销毁的不同阶段）构建全链条的安全防护。IPDRR方法论一般涉及以下阶段：：

- 识别：是整个框架的基础，可以帮助提高组织对系统和数据风险的理解，一般使用数据资产管理，风险评估等技术。
- 保护：可以防止潜在的数据泄露威胁，一般使用身份识别与访问管理，数据防泄漏等技术。
- 检测：数据安全事件可以通过日志审计、持续监控等技术及时发现。
- 响应：可以使用应急响应、缓解等技术来控制事件的影响。
- 恢复：使用数据恢复、改进等技术，可以及时恢复正常运行，以减轻事件的影响。

3. 安全运营体系

数据安全运营的核心价值在于发现、验证、分析、响应和解决数据泄露问题，不断优化安全事件处理能力。对于企业安全来说，安全运营比仅仅部署安全产品更重要。

总结

在国内，合规驱动是企业安全的主要驱动因素。随着《网络安全法》、《数据安全法》、《个人信息保护法》的发布，企业作为合规主体，需要积极履行法律法规要求，加强安全治理，遵循合规标准。

攻击者在利益的驱使下，利用多种手段攻击“高价值”的企业目标，通常会导致企业的数据泄露、业务连续性损害和经济损失。因此，企业在威胁事件的驱动下会加大对企业安全的投入，积极构建能够主动防御DDoS、勒索软件和数据泄露等不同威胁事件的安全能力。

使用面向全局的企业架构设计方法，企业可以更好地进行安全能力设计和构建。本文通过列出大部分企业所面临的国内合规要求及常见的威胁案例，供企业进行参考，从而帮助企业更好地处理信息安全的两难困境。

作者

王宣

印孚瑟斯中国战略技术组负责人

他负责印孚瑟斯在中国的架构师团队，领导团队在企业、解决方案和技术层面发展和优化架构能力，并专注于数字化转型和企业现代化旅程、云迁移、数据分析、机器学习、Web3 和区块链等尖端技术的应用。

赵宁

印孚瑟斯中国高级安全架构师

他主要负责印孚瑟斯在中国的安全业务，聚焦于企业安全、云安全和安全运营等信息安全创新领域。他曾参与多项行业安全标准的制定，具有国际信息系统安全专业认证（CISSP）、国内注册信息安全专业人员（CISP）、数据安全官（DPO）、ISO27001等多项安全认证。

参考：

1. https://pubs.opengroup.org/architecture/togaf9-doc/arch/

For more information, contact askus@infosys.com

Navigate your next