

The background is a dark blue gradient with a complex digital pattern. On the left, there is a circular grid of thin white lines. A bright, multi-colored light streak (yellow, orange, and blue) originates from the center of this grid and extends horizontally across the middle of the image. To the right of the light streak, there are several horizontal bands of blurred, glowing digital data or code, giving a sense of motion and technology.

信息主管

如何推动企业信息安全建设

李炜

自我介绍 - 李炜

☀ 中国卫通集团信息中心主任

☀ 北大CIO班同学会会长

☀ CIO自媒体联盟秘书长

☀ CIO老友汇发起人之一

☀ 中关村大数据产业联盟副秘书长



CIO新思维

职业能力提升之道

△ CIO自媒体小组 编著



电子工业出版社
ELECTRONIC INDUSTRY PRESS
http://www.pke.com.cn

如何推动企业信息安全建设

- ☀ 中国企业信息化建设现状
- ☀ 中国企业信息安全现状
- ☀ 挑战与机遇
- ☀ 信息安全价值分析
- ☀ 从文化等层面推动信息安全建设
- ☀ 信息安全建设原则

中国企业的信息化现状

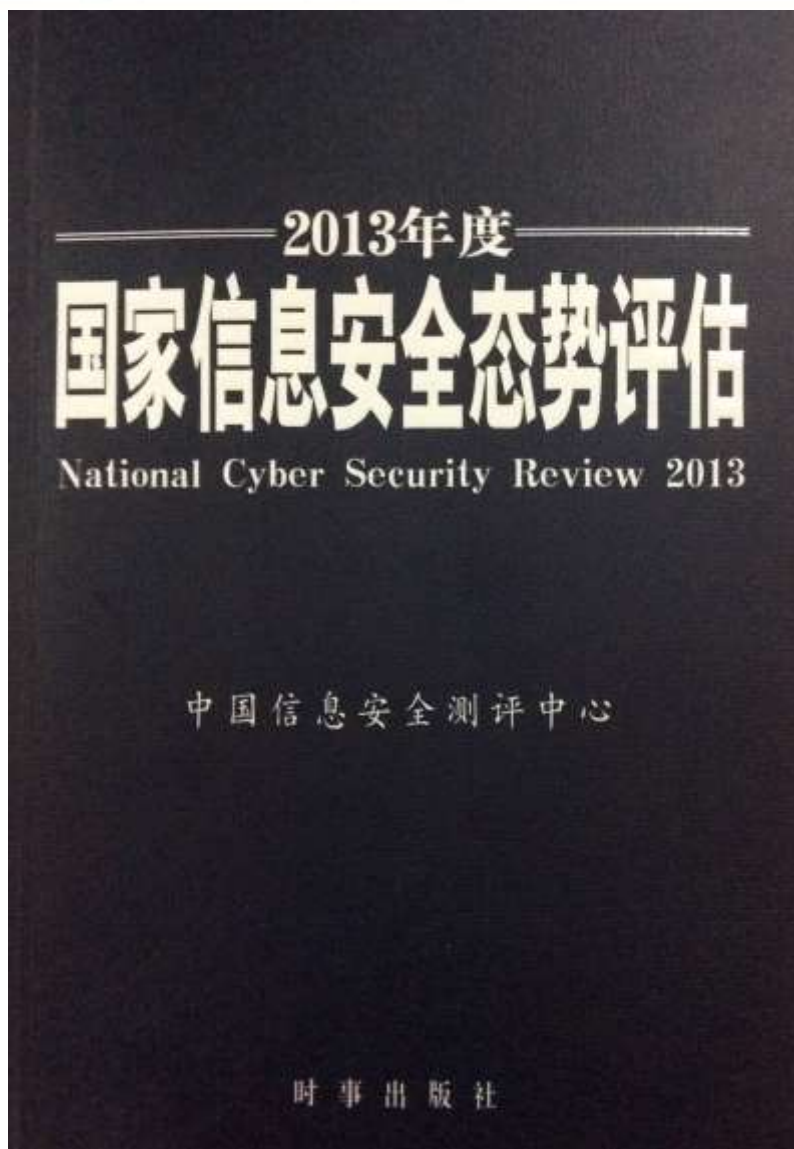
☀️ **中国企业的信息化综合指数不高**

☀️ **中国企业整体信息化成熟度处于中等偏下的状态**

中国企业的信息化现状

- ☀ 中国企业信息化建设和应用缺乏前瞻性，信息技术与实际业务发展的需求匹配度低，在信息化应用范围的广度和深度上远远不够，大多数的信息化应用集中在部分业务中，体现不出整体信息化的效益。
- ☀ 中国企业普遍不重视IT治理，IT制度、IT绩效考核体系、IT部门设置不完善，虽然IT部门承担企业信息化建设和应用的职能，但推动力度欠佳。
- ☀ 企业中高层管理人员参与信息化程度较低，非IT的管理人员较少的参加了信息化的工作，信息化领导力较弱。
- ☀ 信息技术未能充分发挥其在中国企业中的应有价值，对企业发展的贡献不足，对企业提高核心竞争力、提升内外部管理能力、落实创新、助力业务发展、提升市场反应能力和决策支持等方面的贡献仍显微薄，贡献低于预期。

中国企业的信息安全现状



☀ 随着行业新技术新应用的引入、业务多元化的实现以及信息化工业化的不断融合，重要行业和企业的信息安全建设明显滞后于信息化的发展，基础信息网络与重要信息系统的脆弱性依然突出，信息安全风险已升至行业风险的高位，关键数据的安全和业务的连续性面临极大的挑战。

中国企业的信息安全现状

- ☀ 一是行业和企业内部的信息安全发展极不平衡，存在安全短板。
- ☀ 行业间的信息化和信息安全发展有先有后，金融、电力行业和企业的信息安全发展较早，安全防护水平相对较高，但还有部分行业和企业的信息安全的滞后程度相当严重。
- ☀ 企业内部层面，大型企业的特点是规模庞大、机构众多、业务复杂，往往业务和网络覆盖到全国各地甚至海外。下属分支机构的信息安全重视和投入程度不一，因而建设和防护水平参差不齐，系统整体防御和纵深防御体系比较薄弱，导致出现短板效应，极易引发全局性安全问题。

中国企业的信息安全现状

- ☀ 二是数据安全未得到足够重视，敏感数据存在泄露隐患。
- ☀ 没有采取切实有效的数据防外泄的措施，数据没有根据重要程度分类分级进行保护，大量敏感数据采用明文传输和存储，存在泄露隐患。
- ☀ 外部边界特别是互联网出口防护不善，网络隔离不利，应用层的安全漏洞大量存在，导致大量敏感数据面临失窃风险。

中国企业的信息安全现状

- ☀ 三是安全检测和感知能力不足，无法及时发现和处置攻击等异常行为。
- ☀ 虽然部分企业已经部署了入侵检测的设备，但是部署位置不当、规则库老旧、报警日志无人查看等现象普遍存在，入侵检测设备形同虚设。
- ☀ 部分企业应急响应体系和机制仍不健全，缺少实际演练。信息化人力资源和技术能力不足，无法发挥作用。
- ☀ 特别无法应对高级别的攻击和威胁，企业信息安全长期处于被动状态。

中国企业的信息安全现状

- ☀ 四是关键技术受制于人，安全隐患与日俱增。
- ☀ 企业中广泛应用的信息技术产品，从网络核心设备、大型主流软件、核心应用系统到新技术产品，依然是国外的产品，对存在的漏洞和后门无法及时知晓。
- ☀ 部分企业在产品选型中，对信息安全的考量不足，对产品的安全评估、系统上线前的安全测试不够重视，带来较大安全风险和隐患。

中国企业的信息安全现状

- ☀ 五是安全规划和建设未能同步，新技术的风险不断引入。
- ☀ 随着云计算、大数据、移动应用的普及，不少企业在积极跟进新技术的步伐。
- ☀ 在应用新技术的同时，部分企业没有充分考量安全问题，对安全规划和建设未能同步进行，在没有进行安全风险评估、未落实安全保障措施的情况下，强行上线云平台、移动办公系统等等，导致新技术和新应用带来了新的安全风险和隐患。

中国企业的信息安全现状

☀️中国企业的信息安全形势不容乐观！

☀️信息安全保障能力无法满足信息化的发展需求！

挑战与机遇

☀️差距：目标和方向；不足：发展空间。

☀️挑战与机遇并存！契机：

☀️国家对信息安全的重视前所未有，历史性机遇。

☀️企业越来越认识到信息安全是企业可持续性发展的一个基本要求。

历史机遇

- ☀ 2014年2月27日，中央网络安全和信息化领导小组宣告成立，在北京召开了第一次会议。机构职责：
- ☀ 着眼国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题；
- ☀ 研究制定网络安全和信息化发展战略、宏观规划和重大政策；
- ☀ 推动国家网络安全和信息化法治建设，不断增强安全保障能力。
- ☀ 表明了保障网络安全、维护国家利益、推动信息化发展的决心。

信息安全对企业的价值

- ☀ 一是保护企业客户信息和内部组织信息。企业的客户信息、商务伙伴的资料和数据，以及企业内部的组织信息、员工信息，都是企业赖以生存的基础，是需要保护的主要资产。
- ☀ 二是保护基于互联网的商务活动过程和数据。电子商务是当前世界商务活动运作发展的主流方向，越来越多的企业已经在大量的利用电子商务来取代传统的商务活动。这种通过互联网，以电子数据交换为主要方式的活动必须加以保护，以避免信息泄露、信息篡改、身份欺诈等行为给企业造成的纠纷和困扰。

信息安全对企业的价值

- ☀ 三是保护企业商业秘密。现代企业的正常运作已经离不开信息资源的支持。商业秘密的泄露会使企业丧失竞争优势，失去市场。企业要保持可持续性发展，信息安全是最基本的保障之一。
- ☀ 四是保障业务持续运转。“天有不测风云”，像地震、火灾、爆炸等等自然灾害和不可抗力，软硬件故障、病毒木马等等威胁，都会造成企业商务活动的中断，甚至企业的破产。例如911恐怖事件的发生，让很多企业遭受了灭顶之灾。因此，为了防止企业经营活动的中断，保护关键商务过程免受重大故障和灾难的影响，建设安全健壮的信息系统必不可少。

如何推动企业信息安全建设

☀ 信息化三分技术、七分管理

☀ 从系统论的观点，信息系统是一个复杂的系统，是由信息技术系统、系统运行环境和信息组成，不仅包括组成信息技术系统的计算机软硬件、网络基础设施、系统平台、通信平台，还包括系统运行内外环境中的人、组织、管理、物理环境这些因素。

☀ 而且它们之间是相互影响、相互作用、相互制约的，成为有机联系的整体。

如何推动企业信息安全建设

- ☀信息安全也不是一个单纯的技术问题。
- ☀不仅要考虑到信息安全的技术层面、管理层面的问题，也要考虑到人员层面、文化层面的问题，这几个方面也是相关制约、相互作用、相互影响的。
- ☀必须有全方位的考虑，才能保障信息安全的目标得以实现，也就是保障信息系统和信息的私密性、完整性和可用性。

建立信息安全文化

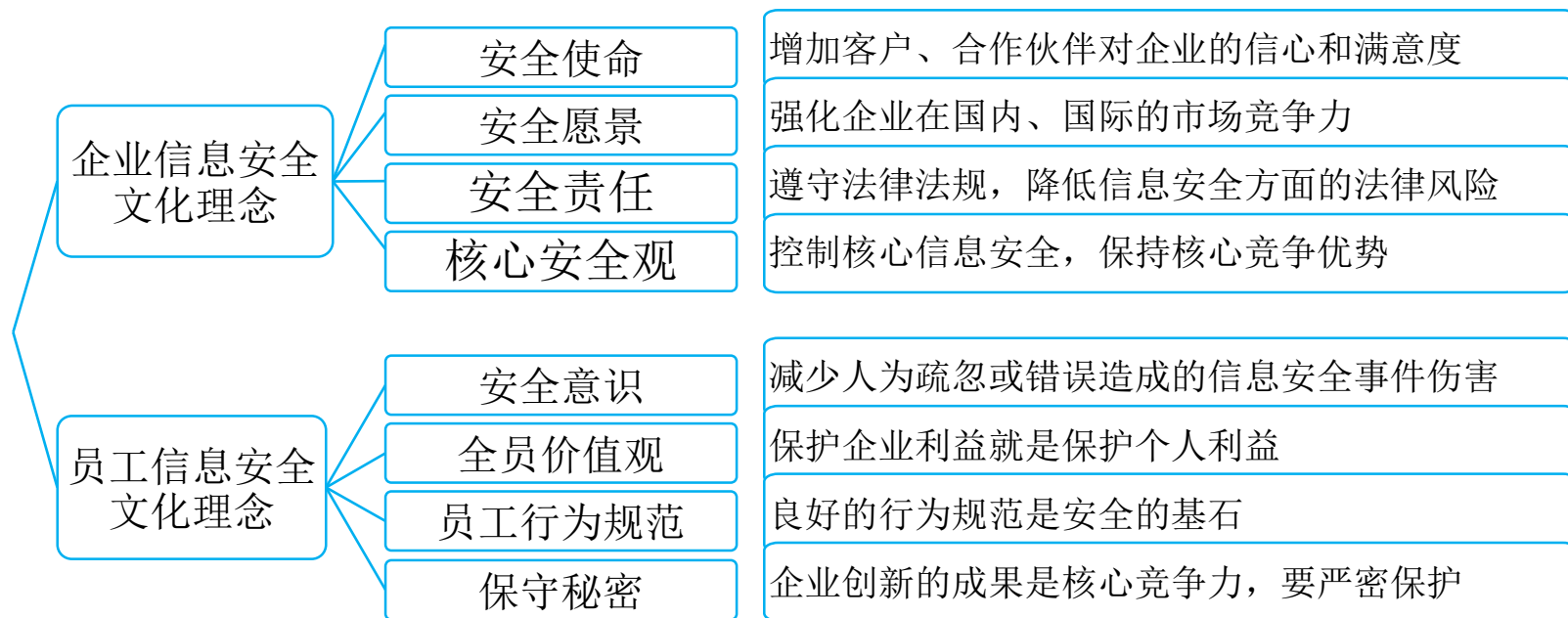
- ☀ 企业文化是企业内的一套通用价值体系，通过企业价值观、承诺、传统等社会特征，无形中约束企业和企业成员的言行，使企业和企业成员的行动向着实现企业发展目标的方向前进。
- ☀ 有时候当技术和管理规章制度不能用来约束每一个行为时，文化能够起到很好的作用。
- ☀ 核电站的“安全文化”：把企业文化和安全结合在一起的典型。四个“凡事”：“凡事有章可循，凡事有人负责，凡事有据可查，凡事有人监督”

建立信息安全文化

- ☀ 核电站的“安全文化”，是国际核能界在三里岛和切尔诺贝利事故后，结合“企业文化”的管理思想，提出的新的安全管理思想和原则，它是传统的纵深防御原则的扩充，也是安全管理思想的一次重大变革。
- ☀ 建立一种信息安全的文化，就是把信息安全看作是企业文化的一个组成部分，把企业文化引入到信息安全管理政策中，直接引导和影响企业员工对待信息安全工作的方式和态度。企业员工对待信息安全的态度、行为和实践一旦形成一种风格、一种习惯，信息安全工作就比较好开展。

某企业信息安全文化

信息安全归根到底是对人的行为管控，良好的信息安全文化理念是企业安全的灵魂，信息安全文化是企业文化的重要组成部分。



建立信息安全文化

☀ 宣贯：

☀ 国内外信息安全形势

☀ 国家信息安全政策

☀ 突出的信息安全事件

☀ 企业信息安全制度

☀ 企业信息安全文化理念

国际信息安全形势

- ☀ 网络空间的政治化、军事化、情报化态势明显，“控制”与“反控制”博弈加剧
- ☀ 网络空间威胁多元复杂，网络攻击案例频发，新技术发展与安全风险交叠激荡，各国纷出重拳强化网络防御
- ☀ 大数据加速网络空间“控时代”来临，数据安全性凸显，“信息供应链”成信息安全的关键
- ☀ 企业在国家信息安全战略链条中的作用凸显，产业“自主可控”诉求席卷全球
- ☀ 全球网络空间外交博弈持续升温，国际合作运筹加大，战略关系构建增强态势

国家政策法规

- ☀ 国资委《中央企业商业秘密信息系统安全技术指引》；
- ☀ 公安部《计算机信息系统安全等级保护基本要求》；《信息安全技术信息系统安全等级保护定级指南》
- ☀ 全国人大《全国人民代表大会常务委员会关于加强网络信息保护的決定》
- ☀ ISO / IEC 27001 : 2005《信息技术安全技术信息安全管理体系要求》和ISO / IEC 27002 : 2005(信息技术安全技术信息安全管理体系实施细则》

中央企业商业秘密信息系统安全技术指引

4.1 中央企业商业秘密保护范围

依据《暂行规定》，中央企业商业秘密的保护范围主要包括：战略规划、管理方法、商业模式、改制上市、并购重组、产权交易、财务信息、投融资决策、产购销策略、资源储备、客户信息、招投标事项等经营信息，设计、程序、产品配方、制作工艺、制作方法、技术诀窍等技术信息。

信息安全事件案例

☀ 入侵大型离子对撞机



☀ 2008年9月10日，黑客侵入 “紧凑介子螺线管实验” 探测器计算机系统，再前进一步就可获得关闭探测器权限，后果将不堪设想

信息安全事件案例

☀ 2010年1月12日，百度公司网站（baidu.com）突然无法访问。

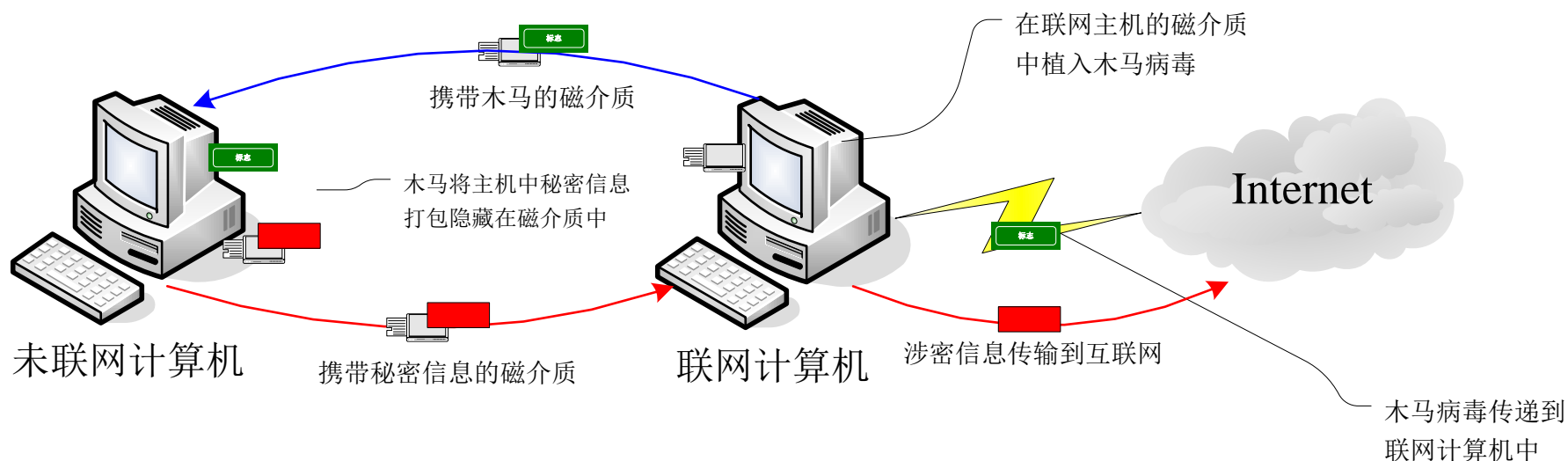


信息安全事件案例

- ☀ 原因是baidu.com域名的注册信息被代号为“伊朗网军”的组织非法篡改，致使baidu.com域名在全球的解析被错误指向，最终导致全球互联网用户无法正常访问baidu.com网站。
- ☀ 互联网中DNS服务器安全性未受到应有的重视，本次事件中，黑客绕开了百度自身的安全保护而选择直接攻击DNS服务器，导致了此次攻击的严重后果。

信息安全事件案例

☀ 与互联网隔离的内部网络面临的安全风险



从组织和人员层面推动

☀ 信息化：一把手工程

☀ 成立由企业主管领导任责任人的信息安全管理机构。职责：

☀ 组织制定信息安全策略、流程和规章制度；

☀ 组织信息安全风险评估和信息安全教育培训；

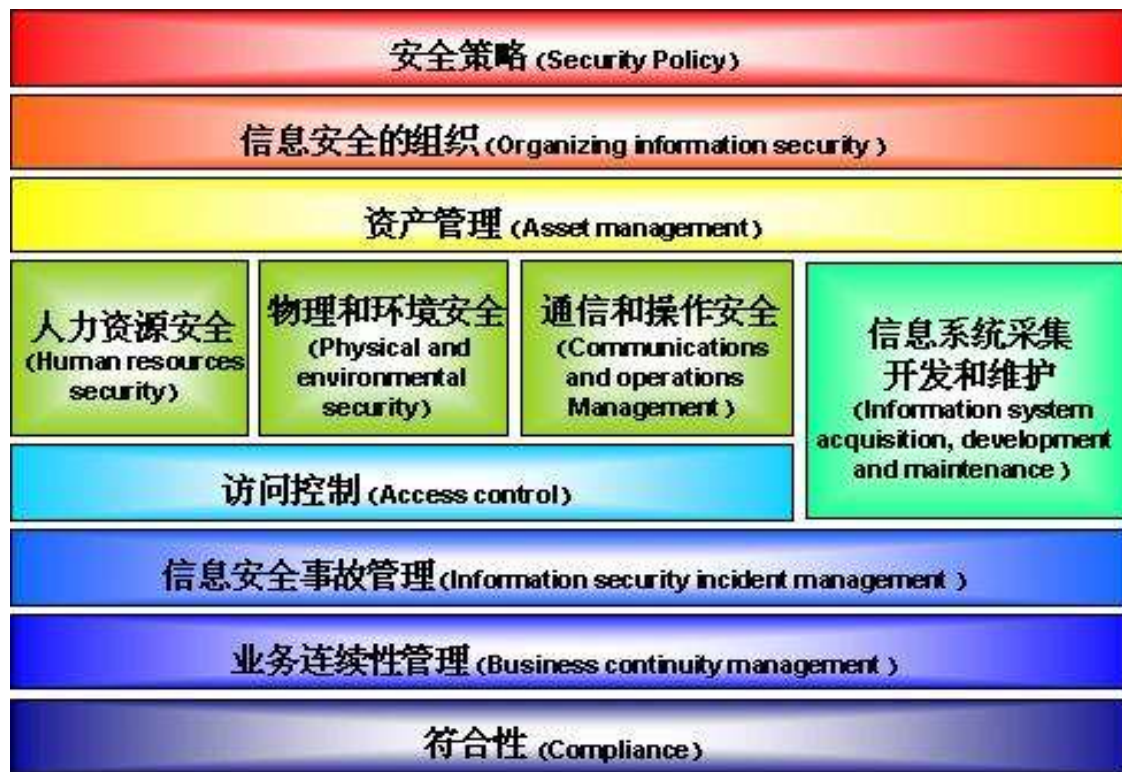
☀ 落实年度信息安全计划、报告等；

☀ 与国家相关主管部门建立日常工作关系；

☀ 执行国家相关法律法规。

信息安全管理 - ISMS国际标准

- ☀ ISMS（信息安全管理），基于业务风险方法，来建立、实施、运行、监视、评审、保持和改进信息安全的。
- ☀ 管理体系包括组织结构、方针策略、规划活动、职责、实践、程序、过程和资源。



信息安全技术体系

- ☀ 物理安全
- ☀ 网络安全
- ☀ 主机系统安全
- ☀ 应用安全
- ☀ 数据安全
- ☀ 灾难备份和恢复
- ☀ 内容安全
- ☀ 终端安全

信息安全建设原则

☀ 信息安全建设原则

☀ 遵循国际、国内、行业信息安全法规、标准；

☀ 注重投入产出比，安全与投资的平衡，业务重要性与防护等级的一致；

☀ 三分技术、七分管理，谁主管谁负责；

☀ 统一性：统一安全策略、统一安全规划、统一安全标准、统一安全建设；

☀ 全面考虑，分步实施。

总结

☀谢谢！

☀敬请批评指正！

☀李炜

☀13810317008@139.com

