企业数字化转型中的信息安全治理能力建设研究

陈治舟
杭州合众数据技术有限公司　浙江　杭州　310000

摘　要：随着社会经济的不断发展，我国企业的发展也迎来了更多的机遇和挑战。近年来，伴随数字技术与实体经济的持续深度融合，越来越多的企业将数字化转型作为企业发展战略的重要组成部分，将技术和数据驱动的理念、方法与运营管理机制嵌入企业变革之中。企业数字化转型是指通过将数字技术引入现有管理架构，推动信息结构、管理方式、运营机制、生产过程的重塑，实现企业运营与管理智能化的过程。借助数字化转型，企业可以驱动商业模式的持续升级，实现降本、增收和提效等具体目标。然而，企业在享受数字化转型所实现的更高商业价值的同时，也面临着日益复杂且严峻的网络和信息安全形势，如频发的数据泄露事件、频繁的网络攻击等。因此，如何防范和控制信息安全风险，确保数字化转型中关键信息资产的安全是企业实践中迫切需要解决的问题。

关键词：企业数字化转型；信息安全治理；对策

引言

在信息化持续发展的今天，信息安全特别是国家层面的信息安全已经上升到国家战略高度。同时，全球经济正在步入数字时代，主要发达国家都在推动企业的数字化转型，以取得主动权和话语权。现阶段，以数据为核心的信息资源是金融、能源、交通、水利、粮食、生态、国防科技工业等重要领域内企业运营管理的基础。如果没有微观层次上企业的信息安全，那么国家层面的信息安全也就无从谈起。然而，伴随企业数字化转型而频繁发生的系统误用、数据泄露、网络攻击、关键信息基础设施遭到破坏、工业互联网服务中断等信息安全事件，不仅在组织层面造成严重的经济损失，而且还威胁到国家层面的信息安全，这也充分暴露了微观层面上企业的信息安全治理缺失所可能造成的严重危害。因此，面对数字化转型中频繁发生的信息安全事件，企业需要快速提升信息安全治理能力，以确保数字化转型中关键信息资产的安全，实现企业的高质量发展。

1 企业信息安全建设的困惑

随着我国信息产业持续高速发展，企业的信息化建设已经进入到“建设应用并重，着力深化应用”的阶段。企业内部信息系统在纵向、横向两个方面耦合程度日益加深，系统间的相互联系日益增强。为保障企业信息系统安全、持续、可靠、稳定运行，企业在信息安全方面投入了很多资源，包括建立一定的安全管理规范、制度和流程，采取通用或专用的安全防护技术和产品进行落实，等等。但是通常企业领导和信息安全主管还存在一系列的困惑。比如，企业在安全方面投入了较多的资源，但仍不时有安全方面的问题困扰。为什么付出了很多的资源代价，实施了安全管理却没有达到最初的安全管理目标？是因为技术层面上资金投入不够，还是管理落实上难以实现，或者是公司层面上对信息安全风险理解得不透彻？做安全项目制定一大堆的制度，写了一大堆的文档，如何能真正地执行下去？这都需要管理者深入思考。

2 企业信息安全治理能力的特点

（1）企业信息安全治理能力受到信息安全治理体系的影响。企业信息安全治理结构、治理机制与治理模式可以看作是企业开展信息安全相关活动的重要资源，这三种治理要素也构成了相对完整的企业信息安全治理体系。企业信息安全治理体系所体现出来的能力就是信息安全治理能力，这种能力与信息安全治理结构中领导者的个人能力、治理机制中的具体工具以及企业内部的信息安全治理环境等要素紧密相连。这些要素相互影响、相互作用，并综合地表现为信息安全治理能力。（2）企业信息安全治理能力具有动态性。一方面，伴随企业对大数据、云计算、物联网等数字技术的采纳，对企业信息安全提出了新的更高的要求。因此，企业信息安全治理所针对的风险场景不是一成不变的，它们始终处在不断变化的动态过程中，这就使得企业信息安全治理能力需要满足这种动态性的变化。另一方面，企业数字化转型下的信息安全几乎涉及所有部门、流程与业务单元，这就决定了信息安全治理是一项复杂的系统工程，需要及时根据业务变化动态培养、匹配对应的信息安全治理能力。（3）企业信息安全治理能力需要适配数字化转型进程。企业信息安全从来不是绝对的，而是相对的，绝对化的企业信息安全状态几乎不存在。企业对于信息安

全的追求如果超过某个限度，成本就会显著上升，收益自然也会下降，进而导致数字化转型不仅没有带来“降本、增收、提效”的效果，反而成为企业负担。因此，面向企业数字化转型的信息安全治理能力要适配数字化转型进程，既要避免超前部署造成的巨大成本压力，又要避免滞后跟进导致的巨大信息安全风险。

3 信息安全问题

目前企业信息安全问题主要包括几个方面。（1）信息质量低下：无用信息、有害信息或劣质信息渗透到企业信息资源中，对信息资源的收集、开发和利用造成干扰。（2）信息泄漏：网络信息泄漏和操作泄漏是目前企业普遍存在的信息安全困扰。网络信息泄漏是信息在获取、存储、使用或传播的时候被其他人非法取得的过程。而操作泄漏则是由于不正当操作或者未经授权的访问、蓄意攻击等行为，从而使企业信息泄漏。（3）信息破坏：指内部员工或者外部人员制造和传播恶意程序，破坏计算机内所存储的信息和程序，甚至破坏计算机硬件。（4）信息侵权：指对信息产权的侵犯。现代信息技术的发展和应用，导致了信息载体的变化、信息内容的扩展、信息传递方式的增加，虽然实现了信息的全球共享，但同时也带来了知识产权难以解决的纠纷。

4 企业信息安全建设的目标

企业信息安全治理是一个针对未知威胁由被动预防性管理转变为主动风险监管的过程。在这一过程中，需要对未来所面临的威胁和漏洞进行合理主动的评估，并采取相应的危险防范预案，借助对监管资源的合理配置最大化实现信息安全保障工作的顺利进行。在企业内部进行安全防控过程中需引入科学的管理手段，并在PDCSA环的帮助下，进行动态化监管与治理，借助信息治理流程实现资源的合理配置，最大化推动关键性技术、关键性项目、关键性措施的开展。在企业范围内实现信息安全治理要完成五个方面的目标。第一，实现价值交付，具体体现在提供信息安全承诺，将信息安全管理成本降低，提高企业的业务可靠性。第二，资源管理，对信息运行的重要资源进行优化和管理。第三，实现绩效度量，借助科学的手段对信息安全管理弥补和信息资源投入情况做出合理规划，并对执行的具体过程进行实时跟踪。第四，实现风险管理，要求企业内部人员具有较强的风险意识和风险防范意识，充分分析与认识组织遇到的关键性风险，并在下一过程即组织结构涉及中具体明确指派风险责任。第五，整体治理战略保持一致，要求设计信息安全计划，组织整体计划以及详细业务目标这三个层面形成关联。

5 企业信息安全治理能力建设的对策

5.1 建立健全企业信息安全治理体系

针对企业数字化转型对信息安全提出的新要求，企业需要建立能适应数字化转型发展的信息安全治理体系。具体而言，数字化转型会对企业的组织结构、形态和功能产生影响，组织结构趋向于打破层级的扁平化，追求灵活且敏捷地适应外部市场变化。据此，企业信息安全治理结构要明确不同相关主体的权责利关系，构建信息安全分权治理结构。以企业内部信息安全有序运作为目标，完善企业的制度安排和关系协调机制，从合规、契约、关系和流程等不同维度逐步完善企业信息安全治理机制。及时跟踪企业信息安全治理实施过程中具体岗位的信息安全风险处置和责任落实情况，结合不同流程与岗位之间的信息安全风险责任对接情况，不断改进企业信息安全治理模式。最终，通过治理结构、治理机制和治理模式的不断完善和良性互动，逐步建立健全企业信息安全治理体系。

5.2 设计合理的信息安全治理结构

企业信息安全治理是一项复杂的系统工程，需要综合考虑企业高层管理团队中CEO、CIO、CFO、各部门主管，以及广大员工的利益、诉求和责任。在秉承多元治理主体的理念下对信息安全治理相关的决策权、执行权、投资权、监督权等权利进行合理配置，完善企业信息安全治理的治理结构。加强企业信息安全治理数字化转型，实现信息安全与数字化转型战略的良性互动与匹配。

5.3 提高企业员工的网络与信息安全意识

企业信息安全问题，三分是技术问题，七分是管理问题，科学合理的信息安全管理制度和严格的执行是企业信息安全的保障。由企业信息安全风险的主要来源可知，持续提升企业内部员工的网络与信息安全意识在企业数字化转型中尤为重要。从具体措施上来看，企业首先要加强员工的信息安全教育，帮助员工树立正确的信息安全意识，并辅以适当的奖惩措施让信息安全深入员工日常工作之中。其次，企业更新升级数字技术与信息系统之后，要及时为员工开展必要的信息安全技术培训，帮助员工掌握正确的技术设施与信息系统操作方法，最大限度减少不当操作发生的可能性。最后，关注企业新进员工以及离职员工关键时间点的信息安全管理，及时强化员工网络与信息安全意识，降低信息安全风险事件发生的概率。

5.4 信息安全风险控制实施

企业对于信息安全风险的控制实施要首先对企业进行风险管理差距分析，建立风险管理标准，并有针对性

的进行风险评估方案设计，风险处置方案设计和风险管理制度设计。要定期开展风险评估、风险处置和风险控制活动，并将整改活动纳入统一的流程管理。企业信息安全治理是一个长期的系统工程，实施路线要适应企业战略和发展需要，确保信息安全相关管理措施和技术手段适应企业的目标和文化，并与之协调一致。要准确把握当前和未来一定时期内信息系统所面临的威胁和风险，用适当的投入有效管控所有的威胁和风险。企业信息安全治理以企业运行流程为依托，结合信息安全管控点，将管控流程与组织机构相对应。确保企业信息安全知识库、架构、平台和工具有效使用，测量、监控和审计管控手段和流程，确保安全管控的目标完成和实现。最终通过适当安全投入，有效的安全项目的实施和交付，确保企业业务发展的目标实现。

5.5 提高企业信息安全治理能力的智能化水平

企业数字化转型以业务流程的数据化与自动化为基础，通过大数据、云计算与人工智能等数字技术，最终实现运营与管理的数字化与智能化。数字化的手段也能够提升企业信息安全治理能力，表现如下：第一，基于企业内部数据库，实现业务流程智能优化的同时可以嵌入信息安全监控措施，高效管理并监控信息安全风险，维护自动化业务流程的安全运行；第二，基于人工智能技术，对企业数字化业务流程系统不断优化，实现IT基础架构安全管控手段的全面升级，大数据分析与可视化技术，实现企业数据赋能的风险评估、风险预警与风险应对，维护企业安全可信的运营与管理环境；第三，利用数字技术，建立常态化信息安全风险监测机制，及时收集并整理信息安全风险的类型与特点，有针对性地制定信息安全风险防控措施。

结语

当今时代的主题是信息化、智能化，并将相关的技术和理念融入企业和各个领域，从而建立高效、稳定的综合信息管理系统。但随着信息风险的出现，防范风险的企业信息综合管理也逐渐提上了日程。

参考文献

[1]甄杰,谢宗晓,林润辉.治理机制、制度化与企业信息安全绩效[J].工业工程与管理,2021,23(3):171-176,191.

[2]魏凯琳,高启耀.大数据供应链时代企业信息安全的公共治理[J].云南社会科学,2019(1):50-56.

[3]张远新.关于企业信息安全隐患排查与治理研究[J].数字通信世界,2020(7):276.

[4]马之力,张华峰,龚波,等.电网企业基于PDCA的信息安全治理提升方法研究与应用[J].信息安全与技术,2021,6(5):87-90.

[5]赵伯琪.浅谈企业信息安全治理框架[J].信息安全与技术,2020,4(5):19-21.

[6]甄杰,谢宗晓,李康宏,等.信息安全治理与企业绩效：一个被调节的中介作用模型[J].南开管理评论,2020,23(1):158-168.