数字化时代下建筑设计信息安全管理研究

路晓娜
邢台市建筑设计研究院有限公司　河北　邢台　054000

摘　要：随着数字化技术的迅猛发展，建筑设计行业正经历着前所未有的变革。数字化技术在提高建筑设计效率与精度的同时，也带来了信息安全管理的挑战。本文旨在探讨数字化时代下建筑设计信息安全管理的现状、面临的挑战以及应对策略，以期为建筑设计行业的信息安全提供理论参考和实践指导。

关键词：数字化时代；建筑设计；信息安全；管理策略

引言

在数字化时代背景下，建筑设计行业广泛采用计算机辅助设计（CAD）、建筑信息模型（BIM）等先进技术，实现了设计过程的数字化与智能化。然而，这些技术的应用也伴随着大量敏感信息的产生与传输，如设计图纸、工程数据、客户信息等。一旦这些信息泄露或被篡改，将对建筑设计企业造成不可估量的损失。因此，加强建筑设计信息安全管理显得尤为重要。

1 数字化时代下建筑设计信息安全管理的现状

1.1 信息安全意识逐渐增强

近年来，随着信息安全事件的频发，建筑设计企业深刻认识到了信息安全的重要性。企业开始将信息安全纳入日常管理的范畴，通过建立完善的信息安全管理制度，明确各级员工的信息安全职责，确保信息安全工作的有序开展。同时，企业还积极开展信息安全培训，提高员工对信息安全的认知水平和防范意识。在培训过程中，企业不仅普及信息安全的基本知识和法律法规，还结合实际案例，深入分析信息安全事件的原因和后果，使员工深刻认识到信息安全对企业和个人的重要性。此外，企业还鼓励员工积极参与信息安全演练，通过模拟真实的信息安全事件，提高员工的应急处理能力和防范技能。

1.2 信息安全技术不断发展

为了应对日益复杂和多变的信息安全威胁，建筑设计企业不断引入先进的信息安全技术。防火墙作为企业信息系统的第一道防线，能够有效阻挡外部网络的非法入侵和攻击。入侵检测系统则能够实时监控网络流量，及时发现并报警潜在的安全威胁。数据加密技术则确保了企业敏感信息在传输和存储过程中的安全性，即使数据被窃取，也无法被轻易解密和利用。除了这些基础的信息安全技术外，建筑设计企业还在不断探索和应用新的技术手段。例如，采用人工智能和机器学习技术来识别和防御未知的安全威胁，利用云计算和大数据技术来加强数据的备份和恢复能力，确保企业信息系统的可靠性和可用性。这些技术的应用有效提升了企业信息系统的安全防护能力，为信息安全提供了有力保障。

2 数字化时代下建筑设计信息安全管理面临的挑战

2.1 外部威胁日益严峻

随着网络技术的飞速发展，网络攻击手段也在不断演变和复杂化。建筑设计企业作为信息密集型行业，其信息系统中存储着大量的设计图纸、项目资料、客户信息等敏感数据，因此成为了黑客攻击的重点目标。黑客可能通过各种手段，如钓鱼邮件、恶意软件、DDoS攻击等，对企业信息系统发起攻击，导致系统瘫痪、数据泄露等严重后果。数据泄露是建筑设计企业面临的一大风险。一旦设计图纸、项目计划等核心数据被泄露，不仅可能给企业带来经济损失，还可能影响企业的声誉和竞争力[1]。此外，黑客还可能利用泄露的数据进行进一步的网络攻击或诈骗活动，对企业和客户造成更大的损失。除了黑客攻击外，病毒入侵也是建筑设计企业面临的一大威胁。病毒可能通过电子邮件、下载的文件、外部存储设备等途径进入企业信息系统，破坏系统文件、窃取数据或占用系统资源，导致系统运行缓慢甚至崩溃。

2.2 内部风险不容忽视

除了外部威胁外，建筑设计企业还面临着来自内部的风险。员工是企业信息安全的第一道防线，但同时也是信息安全漏洞的主要来源。员工疏忽、故意泄露信息、非法操作等行为都可能导致信息安全事件的发生。员工疏忽是内部风险中常见的一种。由于员工对信息安全意识不足或操作失误，可能导致敏感数据被泄露或系统被攻击。例如，员工可能会在不安全的网络环境下访问企业信息系统，或者将含有敏感信息的文件随意存放在公共云盘上。此外，故意泄露信息也是内部风险中不可忽视的一种。某些员工可能因个人利益或恶意动机，

故意将企业敏感信息泄露给外部人员或竞争对手，对企业造成重大损失。非法操作也是内部风险中的一种。员工可能未经授权访问或修改企业信息系统中的数据，或者利用系统漏洞进行非法活动。这些行为不仅违反了企业的信息安全管理制度，也可能触犯法律法规，给企业带来法律风险。另外，企业内部信息系统可能存在漏洞和安全隐患。这些漏洞可能被黑客利用，进行攻击和入侵。因此，企业需要定期对信息系统进行安全检查和漏洞扫描，及时发现并修复漏洞，确保系统的安全性。

2.3 法律法规要求日益严格

随着信息安全法律法规的不断完善，建筑设计企业需要遵守更加严格的合规要求。如《网络安全法》、《个人信息保护法》等法律法规对企业信息安全管理提出了明确要求。《网络安全法》要求企业建立健全网络安全保护制度，采取技术措施和其他必要措施，保障网络安全，防止网络攻击、侵入、干扰和破坏，维护网络数据的完整性、保密性和可用性。这意味着建筑设计企业需要加强网络系统的安全防护，确保系统不受外部攻击和内部非法操作的威胁。《个人信息保护法》则要求企业处理个人信息应当遵循合法、正当、必要的原则，明示处理信息的目的、方式和范围，并经当事人同意。对于建筑设计企业来说，这意味着需要加强对客户信息的保护，确保客户信息的合法收集、使用和存储，避免信息泄露和滥用[2]。为了满足这些法律法规的要求，建筑设计企业需要建立健全的信息安全管理制度和流程，加强对员工的信息安全培训，提高员工的信息安全意识，确保企业的合规运营。同时，企业还需要定期对信息系统进行安全审计和风险评估，及时发现并解决潜在的信息安全问题。

3 数字化时代下建筑设计信息安全管理的应对策略

3.1 加强信息安全意识培养

信息安全意识是信息安全管理的基石。首先，企业应定期举办信息安全培训。这些培训应涵盖信息安全的基本概念、常见威胁、防范措施等方面，使员工全面了解信息安全的重要性。培训形式可以多样化，如线上课程、线下讲座、互动问答等，以适应不同员工的学习需求和习惯。同时，企业应鼓励员工积极参与培训，将信息安全知识纳入员工绩效考核体系，以激励员工主动学习和提升。其次，企业应制定明确的信息安全政策。这些政策应明确规定员工在信息处理过程中的职责和义务，以及违反政策可能面临的后果。通过政策的引导和约束，使员工自觉遵守信息安全规定，形成良好的信息安全习惯。此外，企业还应积极营造信息安全文化。信息安全文化是企业文化的重要组成部分，它强调信息安全是企业每个人的责任，需要全体员工共同参与和维护。企业可以通过举办信息安全知识竞赛、设立信息安全宣传栏等方式，增强员工对信息安全的认同感和归属感，形成良好的信息安全氛围。最后，企业应鼓励员工积极参与信息安全工作。员工是信息安全管理的直接参与者，他们的积极性和主动性对信息安全工作的成效至关重要。企业可以通过设立信息安全建议箱、鼓励员工提出信息安全改进意见等方式，激发员工的参与热情，共同推动信息安全工作的深入开展。

3.2 引入先进的信息安全技术

技术是信息安全管理的重要支撑。建筑设计企业应积极引入先进的信息安全技术，提高信息系统的安全防护能力。防火墙是信息安全的第一道防线。企业应部署高效的防火墙系统，对进出网络的数据包进行过滤和监控，阻止未经授权的访问和攻击。同时，防火墙还应具备入侵检测和防御功能，能够及时发现并应对网络攻击行为。入侵检测系统是信息安全的重要组成部分。企业应部署入侵检测系统，对网络流量进行实时监控和分析，及时发现异常行为和潜在威胁。一旦检测到入侵行为，系统应立即报警并采取相应的防御措施，如阻断攻击源、隔离受感染系统等。数据加密是保护敏感信息的重要手段。企业应对存储和传输的敏感数据进行加密处理，确保数据在未经授权的情况下无法被读取和使用[3]。同时，企业还应采用强密码策略，要求员工定期更换密码，并使用复杂且不易猜测的密码组合。此外，企业还应定期对信息系统进行安全评估和漏洞扫描。通过安全评估，企业可以了解信息系统的安全状况，发现存在的安全隐患和漏洞。通过漏洞扫描，企业可以及时发现并修复系统中的漏洞，防止攻击者利用漏洞进行攻击。

3.3 建立健全的信息安全管理制度

制度是信息安全管理的重要保障。建筑设计企业应建立健全的信息安全管理制度和流程，确保信息处理的规范性和安全性。首先，企业应明确各部门和岗位的职责和权限。通过明确职责和权限，使各部门和岗位能够各司其职、各负其责，共同维护信息安全。同时，企业还应建立责任追究机制，对违反信息安全规定的行为进行严肃处理，以儆效尤。其次，企业应制定严格的信息安全政策和标准。这些政策和标准应涵盖信息处理的各个方面，如信息分类、存储、传输、使用、销毁等。通过制定政策和标准，规范员工的信息处理行为，确保信息的机密性、完整性和可用性。此外，企业还应建立信息安全审计机制。定期对信息系统进行审计，检查系统

是否符合信息安全政策和标准的要求，是否存在安全隐患和漏洞。通过审计，企业可以及时发现并纠正存在的问题，提高信息系统的安全性。同时，企业还应加强对外包服务和第三方合作的信息安全管理。在与外包服务商和第三方合作伙伴合作时，企业应明确双方的信息安全责任和义务，签订保密协议和安全协议。通过协议约束双方的行为，确保外包服务和第三方合作过程中的信息安全。

3.4 加强与第三方的合作与监管

在数字化时代，建筑设计企业往往需要与第三方合作伙伴共同完成项目。然而，第三方合作伙伴的信息安全状况和能力直接影响着企业的信息安全。因此，企业必须加强对第三方的信息安全监管和合作。首先，企业应与第三方合作伙伴签订保密协议。保密协议应明确规定双方对保密信息的保护义务和责任，以及违反协议可能面临的法律后果。通过签订保密协议，确保第三方合作伙伴在合作过程中严格遵守保密规定，不泄露企业的敏感信息。其次，企业应对第三方合作伙伴进行安全审计。安全审计可以了解第三方合作伙伴的信息安全状况和能力，发现存在的安全隐患和漏洞。通过安全审计，企业可以及时要求第三方合作伙伴整改存在的问题，提高合作过程中的信息安全水平。此外，企业还应关注第三方合作伙伴的信息安全动态。定期与第三方合作伙伴沟通交流，了解其信息安全政策和措施的变化情况，以及可能对企业信息安全产生的影响。通过关注第三方合作伙伴的信息安全动态，企业可以及时调整自己的信息安全策略，确保合作过程中的信息安全。在选择第三方合作伙伴时，企业还应注重其信誉和实力。选择信誉良好、实力雄厚的合作伙伴，可以降低合作过程中的信息安全风险。同时，企业还应与合作伙伴建立长期稳定的合作关系，共同维护信息安全。

3.5 建立应急响应机制

尽管企业采取了多种措施来加强信息安全管理，但仍然无法完全避免信息安全事件的发生。因此，企业必须建立应急响应机制，以应对可能发生的信息安全事件。首先，企业应制定详细的信息安全事件应急预案。应急预案应明确在发生信息安全事件时的报告流程、处理步骤和责任分工。通过制定应急预案，使企业在面对信息安全事件时能够迅速做出反应，减少损失。其次，企业应定期组织数据安全演练和测试[4]。通过演练和测试，可以评估现有安全措施的有效性，发现存在的问题和不足。同时，演练和测试还可以提高员工的应急处理能力和协作效率，使企业在面对真实的信息安全事件时能够更加从容应对。此外，企业还应建立信息安全事件报告机制。一旦发生信息安全事件，企业应立即向相关部门和领导报告，并启动应急预案进行处理。同时，企业还应及时向受影响的客户和合作伙伴通报事件情况，并采取措施减轻其损失。最后，企业还应加强对信息安全事件的跟踪和分析。对发生的信息安全事件进行详细记录和分析，总结经验教训，提出改进措施。通过跟踪和分析，不断完善企业的信息安全管理体系，提高信息安全水平。

结语

数字化时代下建筑设计信息安全管理面临着诸多挑战和机遇。通过加强信息安全意识培养、引入先进的信息安全技术、建立健全的信息安全管理制度以及加强与第三方的合作与监管等措施，建筑设计企业可以有效提升信息安全防护能力，保障企业信息资产的安全和稳定。未来，随着数字化技术的不断发展和完善，建筑设计信息安全管理将迎来更加广阔的发展前景和挑战。

参考文献

[1]王威,曾辉,李特.数字化转型背景下建筑智慧化设计的机遇分析[J].绿色建筑,2024,(06):117-120.

[2]乔梦甜.数字化时代下建筑设计策略探究[J].住宅产业,2024,(10):52-54.

[3]王知亮.建筑设计中数字化技术的应用与效果分析[J].城市建设理论研究(电子版),2024,(27):72-74.

[4]刘丽莎,刘莹.建筑工程设计企业的数字化设计技术应用[J].成组技术与生产现代化,2024,41(02):38-42.