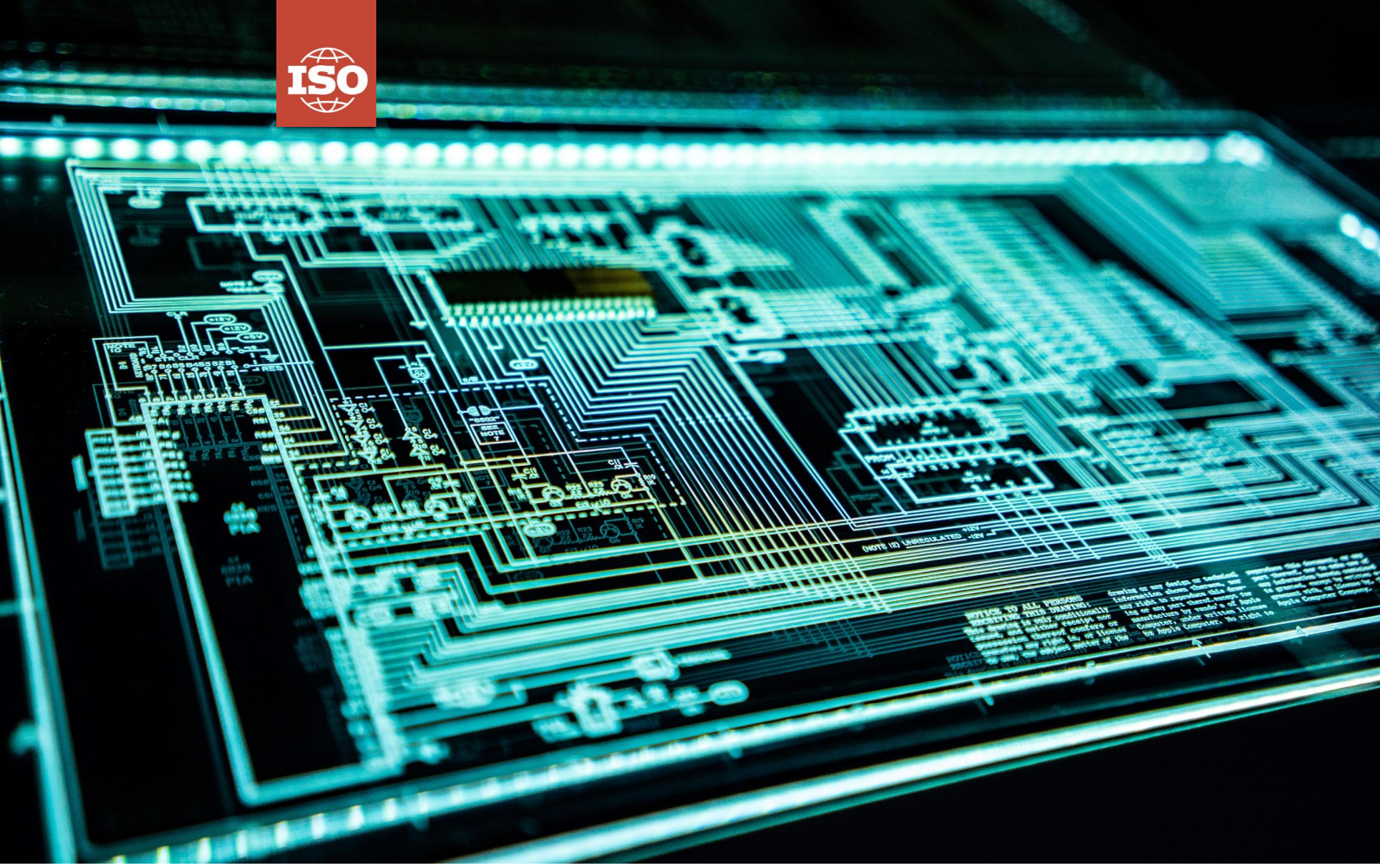


科技巨头如何打造网络复原力

彼此间的不信任把人们推入自我限制的泥沼，但国际标准能让我们自信达观地面对脆弱。

微软、苹果、谷歌、英特尔和 IBM 有什么共同点？除了同属《财富》世界 500 强企业，这些科技巨头都采用了 ISO/IEC 27001 标准。随着该标准在全球数以千计的网站上日益普及应用，它已成为信息安全管理体系的事实标准。

为了防止关键数据资产遭到数字威胁和攻击，各组织机构需要建立网络复原力的理念。网络复原力是技术系统、团队建设、组织文化以及日常运营中不可或缺的一部分。实际上，如今，商业领军人士要比从前更重视网络威胁。世界经济

论坛（WEF）的《2023 年全球网络安全展望》报告指出，有 91%的受访者称，他们认为“至少在未来两年有可能”发生影响深远的灾难性网络事件。

全球企业通过实施 ISO/IEC 27001[1]标准来应对网络安全压力。作为世界上最知名的信息安全管理体系（ISMS）标准，ISO/IEC 27001 是一套有据可依的政策、程序、流程和体系，对网络攻击、黑客入侵、数据泄露和数据盗窃造成的数据损失进行风险管理。

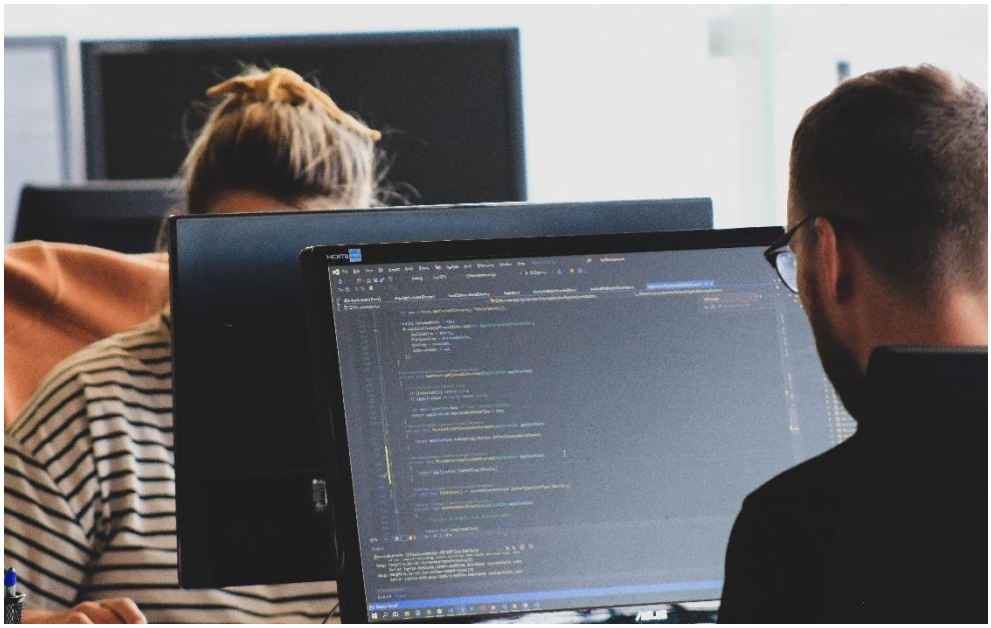
> **各组织机构需要建立网络复原力的理念。**

什么是网络复原力?

网络复原力是指组织机构在遭遇网络攻击或其他网络事件时保持正常运营的能力，一般指具备必要的技术和组织手段，能够监测、应对此类网络事件，并从事件中恢复、吸取经验教训，从而进一步提升复原力。

安德里亚斯·伍尔夫（Andreas Wolf）是 ISO/IEC 信息技术安全标准的专家组牵头人，他说：“网络复原力会在安全预防措施不得力时发挥作用，在数字经济时代，能平稳度过网络中断期的企业才是市场赢家，能化脆弱为力量的机构才敢于冒险。”

[1] ISO/IEC 27001 由 ISO 与国际电工委员会（IEC）共同发布。



伍尔夫对网络安全并不陌生，他带领团队负责 ISO/IEC 27001 标准的更新和修订工作。新版本于 2022 年 10 月发布，旨在应对全球信息技术安全问题，并增强数字信任。该标准鼓励组织机构保护各类信息安全，建立中心化管理框架，减少无效防御技术开支，保护数据的完整性、保密性和可用性，从而增强机构的网络复原力。

然而，网络复原力不单指某个机构的内部运作，而是必须由所有第三方和整个供应链上的全体参与者共同努力才能实现。幸运的是，WEF 的另一份报告《网络复原力指数（CRI）：提高组织机构网络复原力》清晰透明地展示了行业、同行和供应链方面的网络复原力实例，为人们提供了参考框架。

CRI 为公私营部门的网络领导者提供了现实中网络复原力最佳实践的通用框架，衡量组织效能的机制，以及价值传递的方法。根据 CRI 的原则，为实现健全的机构网络复原力开展进一步实践，就是采用公认的安全框架以及 ISO/IEC 27001 等行业标准。

> **在数字时代，我们绝不能在网络复原力上妥协。**

脆弱性是复原力的基础

对竞争对手和政策制定者公开内部运作、分享信息会让很多机构没有安全感，然而恰恰是这种脆弱性才能带来真正的协作和进步。

在数字时代，我们绝不能在网络复原力上妥协。商业实践中也有案例表明，能够自信地面对薄弱环节、积极增强网络复原力的机构，都迅速地成长为了行业领头羊，并开始制定其生态系统标准。ISO/IEC 27001 的整体性方法不仅涵盖信息技术，更覆盖了整个机构，人员、技术和流程都能从中受益。